

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-153072

(43)Date of publication of application : 11.06.1996

(51)Int.Cl.

G06F 15/00

G09C 1/00

H04L 9/06

H04L 9/14

(21)Application number : 07-255169

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 02.10.1995

(72)Inventor : OKAMOTO TOSHIO
SHINPO ATSUSHI
ISHIYAMA MASAHIRO

(30)Priority

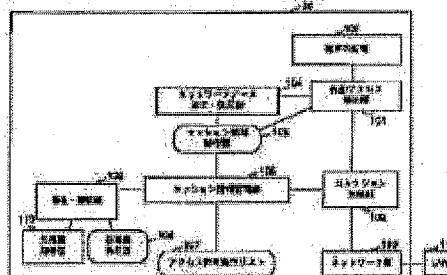
Priority number : 06261277 Priority date : 30.09.1994 Priority country : JP

(54) COMPUTER SYSTEM AND COMPUTER SYSTEM MANAGING METHOD

(57)Abstract:

PURPOSE: To allow a user to operate a computer without caring about difference between the managing methods of the computer that he/she actually uses and the computer of an access object by providing the system with a specified managing means and a memory means storing access permission data generated by this managing means.

CONSTITUTION: This system judges whether or not an access request from a user to each computer in another computer should be permitted, generates access permission data necessary for inspecting whether or not communication to each computer is from a user at a computer which is permitted to access each computer by one user from there, and stores it in a memory. And, access is permitted based on this. Then, a session information managing part 106 manages access from outside so that communication only from a right user outside can be executed. A session information storage part 105 stores data on a session which is permitted to access from the outside by the session information managing part 106.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-153072

(43) 公開日 平成8年(1996)6月11日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0 B	9364-5L		
	C	9364-5L		
G 0 9 C 1/00		7259-5J		C8-19
H 0 4 L 9/06				C8-19
			H 0 4 L 9/02	Z C8-19
審査請求 未請求 請求項の数19 O L (全 31 頁) 最終頁に続く				

(21) 出願番号 特願平7-255169

(22) 出願日 平成7年(1995)10月2日

(31) 優先権主張番号 特願平6-261277

(32) 優先日 平6(1994)9月30日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 岡本 利夫

神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

(72) 発明者 新保 淳

神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

(72) 発明者 石山 政浩

神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

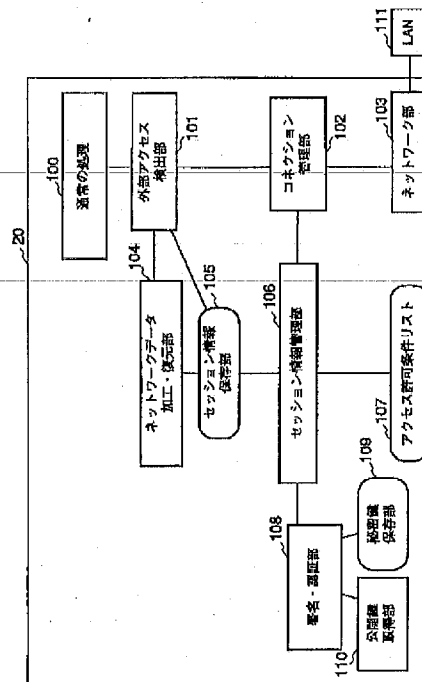
(74) 代理人 弁理士 三好 秀和 (外3名)

(54) 【発明の名称】 計算機システム及び計算機システム管理方法

(57) 【要約】 (修正有)

【課題】 互いに独立した複数の計算機がネットワークを介して接続された環境において、ユーザが実際に使用する計算機とアクセス対象の計算機との管理方法の違いを意識することなく操作できること。

【解決手段】 他の計算機におけるユーザから各計算機へのアクセス要求が許可されるべきかどうか判断し、各計算機への通信がそこからあるユーザによる各計算機へのアクセスが許可されたある計算機におけるあるユーザからのものかどうか検査するのに必要なアクセス許可データを生成し、アクセス許可データをメモリに記憶し、かつそれに基づいて、各計算機へのアクセスが直接的になされたものか、通信手段を介して他の計算機から間接的になされたものかを検出し、後者の場合、アクセスが正当であるかどうかを判定してアクセスを許可する。



【特許請求の範囲】

【請求項1】 複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、他の計算機におけるユーザから該少なくとも一つの計算機へのアクセス要求が許可されるべきかどうか判断し、数少なくとも一つの計算機への通信がそこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成する管理手段と、該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、を有することを特徴とする計算機システム。

【請求項2】 前記少なくとも一つの計算機は更に、前記複数の計算機のどの計算機におけるどのユーザが前記少なくとも一つの計算機にアクセスすることを許可されるべきかを示すアクセス許可条件を格納する格納手段を有し、該アクセス許可条件は前記少なくとも一つの計算機における前記あるユーザのユーザ識別情報を指定し、前記管理手段は該格納手段に格納された該アクセス許可条件に基づいて、該アクセス許可条件を前記アクセス要求が示す前記少なくとも一つの計算機における前記ユーザのユーザ識別情報と比較することにより判断することを特徴とする請求項1記載の計算機システム。

【請求項3】 前記アクセス許可条件は更に前記ある計算機のシステム識別情報を指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機のシステム識別情報と比較することにより判断することを特徴とする請求項2記載の計算機システム。

【請求項4】 前記アクセス許可条件は更に前記ある計算機における前記あるユーザの一時的パスワードを指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機における前記ユーザの一時的パスワードと比較することにより判断することを特徴とする請求項2記載の計算機システム。

【請求項5】 前記アクセス許可条件は更に前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記少なくとも一つの計算機における前記ユーザのユーザ識別情報及び該有効期間を含んだ前記アクセス許可データを生成することを特徴とする請求項2記載の計算機システム。

【請求項6】 前記アクセス要求は、発信元システム識別情報、発信先システム識別情報、及びシステム識別署名データを示し、前記管理手段は該システム識別署名データを認証することにより判断することを特徴とする請求項1記載の計算機システム。

【請求項7】 前記少なくとも一つの計算機は更に、前記少なくとも一つの計算機における前記あるユーザのユーザ識別情報を示すアクセス許可条件を格納する格納手段を有し、前記アクセス要求は、発信先ユーザ識別情報及びユーザ識別署名データを示し、前記管理手段は該ユーザ識別署名データを認証し、該発信先ユーザ識別情報を該格納手段に格納された該アクセス許可が示す該ユーザ識別情報と比較することにより判断することを特徴とする請求項1記載の計算機システム。

10 【請求項8】 前記アクセス要求は更に、発信元ユーザ識別情報も示し、前記ユーザ識別署名データは、前記発信元ユーザ識別情報と前記発信先ユーザ識別情報を前記ユーザの秘密鍵を使って暗号化して求められたものであり、前記管理手段は該ユーザ識別署名データを前記ユーザの公開鍵を使って復号化することにより認証することを特徴とする請求項7記載の計算機システム。

20 【請求項9】 前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機のシステム識別情報及び前記他の計算機における前記ユーザのユーザ識別情報を含んだ前記アクセス許可データを生成することを特徴とする請求項8記載の計算機システム。

【請求項10】 前記アクセス許可条件は更に前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を更に含んだ前記アクセス許可データを生成することを特徴とする請求項9記載の計算機システム。

30 【請求項11】 前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機から前記ユーザによる前記各計算機への通信に使われる鍵データを含んだ前記アクセス許可データを生成することを特徴とする請求項1記載の計算機システム。

【請求項12】 前記少なくとも一つの計算機が更に、該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを前記メモリ手段に記憶した前記アクセス許可データに基づいて判定し、正当と判定された場合、該アクセスを許可する検出手段と、を有することを特徴とする請求項1記載の計算機システム。

40 【請求項13】 前記メモリ手段は、前記ある計算機における前記あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報との組を記憶し、前記検出手段は、前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を前記メモリ手段が記憶しているとき、前記アクセスを正当と判定することを特徴とする請求項12記載の計算機システム。

50

【請求項14】 前記メモリ手段は更に、前記ある計算機における前記あるユーザのための前記アクセス許可データに対応する鍵データを記憶し、

前記少なくとも一つの計算機は更に、前記検出手段が該アクセス許可データに基づいて前記アクセスを正当と判定したとき、前記アクセスの通信データを前記鍵データを使って加工するデータ加工手段を有することを特徴とする請求項12記載の計算機システム。

【請求項15】 前記メモリ手段は更に、前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を記憶し、

前記検出手段は、該メモリ手段に記憶した該有効期間に基づいて、前記アクセスを正当と判定することを特徴とする請求項12記載の計算機システム。

【請求項16】 複数の計算機群が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機群のうち少なくとも一つの計算機群が、

他の計算機群の計算機におけるユーザから該少なくとも一つの計算機群の計算機へのアクセス要求が許可されるべきかどうか判断し、該少なくとも一つの計算機群の計算機への通信がそこからあるユーザによる該少なくとも一つの計算機群の計算機へのアクセスが許可されたある計算機群の計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成するデータ管理サーバと、

前記データ管理サーバにより生成された該アクセス許可データに対応して鍵データを記憶するメモリ手段と、該少なくとも一つの計算機群の計算機へのアクセスが該少なくとも一つの計算機群において直接的になされたものか、前記通信手段を介して他の計算機群の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを前記メモリ手段に記憶した前記アクセス許可データに基づいて判定し、正当と判定された場合、該アクセスを許可する検出手段と、前記検出手段が前記アクセス許可データに基づいて前記アクセスを正当と判定したとき、前記アクセスの通信データを前記鍵データを使って加工するデータ加工手段と、を含むセキュリティゲートウェイと、を有することを特徴とする計算機システム。

【請求項17】 複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムにおける計算機であって、

他の計算機におけるユーザから該計算機へのアクセス要求が許可されるべきかどうか判断し、該計算機への通信がそこからあるユーザによる該計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成する管理手段と、

該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、を有することを特徴とする計算機。

【請求項18】 複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、

該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを判定し、正当と判定された場合、該アクセスを許可する検出手段と、

そこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報と、該あるユーザの該少なくとも一つの計算機における内部ユーザ識別情報との組を記憶するメモリ手段であって、前記検出手段は前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を該メモリ手段が記憶しているとき前記アクセスを正当と判定するものと、

前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データが示すユーザ識別情報を該ユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記内部ユーザ識別情報に変換する変換手段と、を有することを特徴とする計算機システム。

【請求項19】 複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムを管理する方法であって、

他の計算機におけるユーザから各計算機へのアクセス要求が許可されるべきかどうか判断するステップと、該各計算機への通信がそこからあるユーザによる該各計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成するステップと、

該アクセス許可データをメモリに記憶するステップと、該メモリに記憶された該アクセス許可データに基づいて、

該各計算機へのアクセスが該各計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを判定し、正当と判定された場合、該アクセスを許可するステップと、

を含むことを特徴とする計算機システム管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、広域ネットワークに接続され独立管理され、管理の異なる外部からのア

アクセスが制限されている複数の計算機システムを相互に利用するユーザが、外部からのアクセスが許可され、各計算機システムやその管理の違い、例えばユーザIDの違いを意識しないで、自分の個人情報を利用できるユーザ識別情報管理方式を用いた計算機システム及び計算機システム管理方法に関する。

【0002】

【従来の技術】計算機システムの小型化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへと移行している。例えば、オフィス端末やWS（ワークステーション）を設置し、文書作成や表計算処理など事務処理やシミュレーションなどの技術計算に利用し、あるいはCADとして各種設計に利用し、さらには電子メールなどコミュニケーション・システムとして利用している。

【0003】計算機システム自体の進歩に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有やオフィス外のサービスの利用、オフィス外とのコミュニケーションが可能になり、これらが広く利用されはじめた。

【0004】例えば、特殊な処理や高速な処理を要求される科学技術計算のために外部の計算センターにスーパーコンピュータを設置し、それを共同利用している。ユーザは、リモートログイン機能を用いて、自分のWSをスーパーコンピュータに接続し、リモートファイルコピー機能を用いてデータを転送し、処理をスーパーコンピュータで行い、処理結果を自分のWSへ転送し記録媒体への格納やディスプレイへの表示を行うものである。

【0005】また、このようなコンピュータ・ネットワーク環境を利用して、自分のWSを遠隔地のWSと結んでWS会議を行ったり、電子メールを利用して意見を交換することなどが行われている。

【0006】WS会議や電子メールの利用形態では、ユーザがコミュニケーションするのに必要な情報や処理がすべて計算機システム上で実現されている場合には非常に効果大きい。

【0007】さらに、グラフィック技術やファイル容量、マルチメディア技術も進歩してきている。しかし、これに対応する計算機システムやネットワークの機能は不十分である。たとえば、WS会議システムは、内容自体の伝達のためには有効利用し得るが、出席者の微妙な反応、例えば顔色をうかがったり、こちらからの迫力を伝えたりするためには、情報伝達能力が乏しい。TV会議システムのような比較的大規模なミーティングでも、現在の通信能力やWSの表示能力では、参加者各人が小さく表示され、解像度が低く、画面の色再現が悪かったり、動きがなめらかでないなどの問題がある。

【0008】そこで、参加者が所定の会議場所に集まって議論するような従来方式（いわゆる対面方式）おい

て、計算機システムを補助的に用いる形態も良く利用される。そして、会議場所に設置されている計算機システムは、広域ネットワークを介して各参加者が通常利用している計算機システムと接続されていることが通常である。

【0009】しかし、会議場所に設置された計算機システムは、種々の相互に無関係な会議に連続して利用されるので普通であるので、ユーザ名やユーザID、パスワードなどのアカウントの登録は、各会議限りの一時的なものを作成することがある。この場合、参加者は、参加する会議の開催前や会議終了後に、その計算機システムを利用することはできない。さらには、参加者が会議場所の計算機システムから普段利用している計算機システムを遠隔で利用できる場合、後者の計算機システムではユーザの認証ができないので、そのままアクセスを許すには、危険が伴う。

【0010】一方、アカウントを固定的に予め用意しておき、会議に参加するものは、だれでも会議場所に設置された計算機システム利用できるようにする方法も考えられる。この場合、異なる会議の参加者に同じアカウントを重複して割り当てることになるので、会議の前後にもアクセスできるようになるが、同一アカウントを利用する他人のファイルを見ることもできるので、情報の秘匿の点で問題がある。また、このようなアカウントのパスワードは、公開・共有する観点から覚え易いものを用いることが多いので、セキュリティの点でも不利益が生じやすい。

【0011】また、出張先など、組織の異なるところに設置された計算機システムを利用して自分の組織の計算機を利用しようとしても、不正な外部からのアクセスを禁止し、内部の重要な情報を守るために、アクセスを禁止している場合が多い。したがって、外部から自由の自分の組織の計算機システムを利用ができないという不自由さがある。

【0012】

【発明が解決しようとする課題】従来、同一ユーザが、ネットワークを介して接続され、異なる管理下に置かれた複数の計算機それぞれにユーザIDを持ち、ユーザが移動しながら各計算機を使用する場合、各計算機ごとにシステム管理、特にユーザID管理が独立して行われるので、ユーザは、ある計算機に他の計算機を介してアクセスする手続きが非常に面倒であった。また、この手続きを簡略化しようすると、セキュリティの面で問題が生じた。

【0013】また、管理の異なる各計算機間には、通常原則として、外部とネットワークを利用したアクセスは禁止または、非常に厳しく制限された状態になっている。よって、複数計算機を利用するユーザは、ユーザの移動ごとに、必要な計算機とアクセスできるように、ネットワークのアクセス制限を変更する必要があり、その

変更手続きと、変更作業は、非常に面倒であった。

【0014】本発明は、上記事情を考慮してなされたものであり、互いに異なる管理下に置かれた複数の計算機がネットワークを介して接続されて環境において、ユーザが移動しながら各計算機を利用する際に、実際に使用する計算機とアクセス対象の計算機の管理方法の相違を意識することなく操作でき、かつ、相互のネットワーク経由のアクセスを可能にし、かつデータの秘匿性も確保できるユーザ識別情報管理方式を用いた計算機システム及び計算機システム管理方法を提供することを目的とする。

【0015】

【課題を解決するための手段】本発明は、上記の課題を解決するために、ネットワーク上に地理的に分散し、かつ、管理が異なる計算機システム間において、ユーザがアクセスする計算機システムについて、ユーザが直接的にその計算機システムを利用しているか、ユーザが外部計算機システムからリモートでアクセスしているかを検知する。もし、リモート利用の場合、外部計算機システムつまり直接ユーザが利用している計算機システムが、その外部計算機システムでのユーザ管理情報を、リモートアクセス先の計算機システムのユーザ管理情報に反映させることで、ユーザ名やユーザIDの違いによる外部計算機システムからのリモートアクセスの制限をはずすと共にファイル転送やリモートログイン等の時のセキュリティホール（他人の不正利用）を防ぐ。

【0016】また、ユーザが他のマシンを利用した場合、計算機システムごとに異なるユーザIDについて各計算機システムが自動的にユーザIDは違うがユーザ本人は同一というアクセス制御を行い、ユーザIDの差異を吸収するので、あるひとりのユーザが異なる計算機システムを利用しても、自分のファイルに対する適正なアクセスコントロールが自動的に設定されていたり、リモートマシンに存在する同一ユーザのファイルが自動的に転送されたりして、使い勝手が大幅に向上する。

【0017】このために本発明は、基本的には、次のような手段を講じるものである。

・計算機へのユーザ等からのアクセス要求については、そのユーザ等がその計算機を直接利用しているかどうかを検知する。

【0018】・外部からアクセス許可する条件は、同一ユーザに発行された各計算機におけるユーザ識別情報（例えばユーザID）及びその計算機のシステム識別情報（例えばシステムIDや、ネットワークアドレス）間の対応、または、各ユーザ、計算機システムごとに付与されている秘密鍵とそれに対応する公開鍵によって認証可能なユーザまたは計算機システムの署名データによって管理する。

【0019】・外部計算機からのアクセス要求に対しては、その外部計算機のシステム識別情報やユーザ識別情

報、計算機システムやユーザの署名データによる認証などからアクセス要求元を特定し、そのアクセス要求を許可するか否かをアクセス許可条件によって判断する。

【0020】・外部の計算機からのアクセス要求を許可した場合、その許可された通信を識別する情報や、ユーザIDの変換に必要な情報を記憶する。

【0021】・外部の計算機からのアクセスがあると、これが検出され、変換手順を含んだ情報に基づいてデータの変換がなされる。

【0022】・その外部計算機上のユーザ識別情報による操作のデータが、自計算機システム上に届けられると、その外部計算機上のユーザ識別情報による操作は、自計算機システム上のユーザ識別情報からの操作とみなして扱う。

【0023】本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、他の計算機におけるユーザから該少なくとも一つの計算機へのアクセス要求が許可されるべきかどうか判断し、該少なくとも一つの計算機への通信がそこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成する管理手段と、該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、を有することを特徴とする計算機システムを提供する。

【0024】又、本発明は、前記少なくとも一つの計算機は更に、前記複数の計算機のどの計算機におけるどのユーザが前記少なくとも一つの計算機にアクセスすることを許可されるべきかを示すアクセス許可条件を格納する格納手段を有し、前記管理手段は該格納手段に格納された該アクセス許可条件に基づいて判断することを特徴とする。

【0025】又、本発明は、前記アクセス許可条件は前記少なくとも一つの計算機における前記あるユーザのユーザ識別情報を指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記少なくとも一つの計算機における前記ユーザのユーザ識別情報と比較することにより判断することを特徴とする。

【0026】又、本発明は、前記アクセス許可条件は更に前記ある計算機のシステム識別情報を指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機のシステム識別情報と比較することにより判断することを特徴とする。

【0027】又、本発明は、前記アクセス許可条件は更に前記ある計算機における前記あるユーザの一時的パスワードを指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機における前記ユーザの一時的パスワードと比較することにより判断することを特徴とする。

【0028】又、本発明は、前記一時的パスワードは、前記少なくとも一つの計算機にて前記あるユーザに対して予め発行され、前記あるユーザは該少なくとも一つの計算機で発行された該一時的パスワードを指定して前記ある計算機から前記アクセス要求を送信することを特徴とする。

【0029】又、本発明は、前記アクセス許可条件は更に前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記少なくとも一つの計算機における前記ユーザのユーザ識別情報及び該有効期間を含んだ前記アクセス許可データを生成することを特徴とする。

【0030】又、本発明は、前記有効期間は、前記少なくとも一つの計算機にて前記あるユーザにより予め指定された前記あるユーザの個人スケジュールに基づいて決定されたものであることを特徴とする。

【0031】又、本発明は、前記アクセス要求は、発信元システム識別情報、発信先システム識別情報、及びシステム識別署名データを示し、前記管理手段は該システム識別署名データを認証することにより判断することを特徴とする。

【0032】又、本発明は、前記システム識別署名データは、前記発信元システム識別情報と前記発信先システム識別情報を前記他の計算機の秘密鍵を使って暗号化して求められたものであり、前記管理手段は該システム識別署名データを前記他の計算機の公開鍵を使って復号化することにより認証することを特徴とする。

【0033】又、本発明は、前記システム識別署名データは、前記発信元システム識別情報と前記発信先システム識別情報を前記他の計算機の秘密鍵と前記少なくとも一つの計算機の公開鍵を使って暗号化して求められたものであり、前記管理手段は該システム識別署名データを前記他の計算機の公開鍵と前記少なくとも一つの計算機の秘密鍵を使って復号化することにより認証することを特徴とする。

【0034】又、本発明は、前記少なくとも一つの計算機は更に、前記少なくとも一つの計算機における前記あるユーザのユーザ識別情報を示すアクセス許可条件を格納する格納手段を有し、前記アクセス要求は、発信先ユーザ識別情報及びユーザ識別署名データを示し、前記管理手段は該ユーザ識別署名データを認証し、該発信先ユーザ識別情報を該格納手段に格納された該アクセス許可が示す該ユーザ識別情報と比較することにより判断することを特徴とする。

【0035】又、本発明は、前記ユーザ識別署名データは、前記発信先ユーザ識別情報を前記ユーザの秘密鍵を使って暗号化して求められたものであり、前記管理手段は該ユーザ識別署名データを前記ユーザの公開鍵を使

て復号化することにより認証することを特徴とする。

【0036】又、本発明は、前記アクセス要求は更に、発信元ユーザ識別情報も示すことを特徴とする。

【0037】又、本発明は、前記ユーザ識別署名データは、前記発信元ユーザ識別情報と前記発信先ユーザ識別情報を前記ユーザの秘密鍵を使って暗号化して求められたものであり、前記管理手段は該ユーザ識別署名データを前記ユーザの公開鍵を使って復号化することにより認証することを特徴とする。

【0038】又、本発明は、前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機のシステム識別情報及び前記他の計算機における前記ユーザのユーザ識別情報を含んだ前記アクセス許可データを生成することを特徴とする。

【0039】又、本発明は、前記管理手段は前記少なくとも一つの計算機における前記ユーザのユーザ識別情報を更に含んだ前記アクセス許可データを生成することを特徴とする。

【0040】又、本発明は、前記アクセス許可条件は更に前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を更に含んだ前記アクセス許可データを生成することを特徴とする。

【0041】又、本発明は、前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機から前記ユーザによる前記各計算機への通信に使われる鍵データを含んだ前記アクセス許可データを生成することを特徴とする。

【0042】又、本発明は、前記管理手段は更に、前記鍵データを暗号化して前記他の計算機に通知することを特徴とする。

【0043】又、本発明は、前記少なくとも一つの計算機が更に、該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを前記メモリ手段に記憶した前記アクセス許可データに基づいて判定し、正当と判定された場合、該アクセスを許可する検出手段と、を有することを特徴とする。

【0044】又、本発明は、前記メモリ手段は、前記ある計算機における前記あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報との組を記憶し、前記検出手段は、前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を前記メモリ手段が記憶しているとき、前記アクセスを正当と判定することを特徴とする。

【0045】又、本発明は、前記メモリ手段は更に、前記あるユーザの前記少なくとも一つの計算機における内

部ユーザ識別情報を前記外部ユーザ識別情報と外部システム識別情報の組に対応して記憶し、前記少なくとも一つの計算機は更に、前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データが示すユーザ識別情報を該ユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記内部ユーザ識別情報に変換する変換手段を有することを特徴とする。

【0046】又、本発明は、前記メモリ手段は更に、前記外部ユーザ識別情報と外部システム識別情報の組に対応する鍵データを記憶し、前記少なくとも一つの計算機は更に、前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データを該通信データが示すユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記鍵データを使って加工するデータ加工手段を有することを特徴とする。

【0047】又、本発明は、前記メモリ手段は更に、前記ある計算機における前記あるユーザのための前記アクセス許可データに対応する鍵データを記憶し、前記少なくとも一つの計算機は更に、前記検出手段が該アクセス許可データに基づいて前記アクセスを正当と判定したとき、前記アクセスの通信データを前記鍵データを使って加工するデータ加工手段を有することを特徴とする。

【0048】又、本発明は、前記鍵データは前記少なくとも一つの計算機と前記ある計算機とに予め分配されており、前記ある計算機からの前記アクセスの通信データは前記鍵データから生成されたMACを含み、前記検出手段は前記アクセスが正当かどうかを前記メモリ手段に記憶された前記鍵データからMACを生成し、生成されたMACを前記アクセスの通信データに含まれるMACと比較することにより判定することを特徴とする。

【0049】又、本発明は、前記鍵データは前記少なくとも一つの計算機と前記ある計算機とに予め分配されており、前記ある計算機からの前記アクセスの通信データは前記鍵データにより暗号化されており、前記データ加工手段は前記メモリ手段に記憶された前記鍵データを使って前記アクセスの通信データを復号化することを特徴とする。

【0050】又、本発明は、前記メモリ手段は更に、前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を記憶し、前記検出手段は、該メモリ手段に記憶した該有効期間に基づいて、前記アクセスを正当と判定することを特徴とする。

【0051】又、本発明は、前記複数の計算機は各々ユーザ識別情報に基づいて管理されており、前記アクセスが間接的なされた場合に、前記検出手段は更に前記他の計算機が前記少なくとも一つの計算機が管理されているのと同じユーザ識別情報に基づいて管理された計算機であるか、前記少なくとも一つの計算機が管理されているの異なる他のユーザ識別情報に基づいて管理された計

算機であるかを検出し、該アクセスが該他のユーザ識別情報に基づいて管理された計算機からなされたものであるとき該アクセスが正当であるかどうかを判定することを特徴とする。

【0052】更に、本発明は、複数の計算機群が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機群のうち少なくとも一つの計算機群が、他の計算機群の計算機におけるユーザから該少なくとも一つの計算機群の計算機へのアクセス要求が許可されるべきかどうかを判断し、該少なくとも一つの計算機群の計算機への通信がそこからあるユーザによる該少なくとも一つの計算機群の計算機へのアクセスが許可されたある計算機群の計算機における該あるユーザからのものかどうかを検査するのに必要なアクセス許可データを生成するデータ管理サーバと、前記データ管理サーバにより生成された該アクセス許可データに対応して鍵データを記憶するメモリ手段と、該少なくとも一つの計算機群の計算機へのアクセスが該少なくとも一つの計算機群において直接的になされたものか、前記通信手段を介して他の計算機群の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを前記メモリ手段に記憶した前記アクセス許可データに基づいて判定し、正当と判定された場合、該アクセスを許可する検出手段と、前記検出手段が前記アクセス許可データに基づいて前記アクセスを正当と判定したとき、前記アクセスの通信データを前記鍵データを使って加工するデータ加工手段と、を含むセキュリティゲートウェイと、を有することを特徴とする計算機システムを提供する。

【0053】又、本発明は、前記セキュリティゲートウェイは前記検出手段と前記メモリ手段の機能を有するフィルタリングルータと、前記メモリ手段と前記データ加工手段の機能を有するデータ処理サーバとに分離されていることを特徴とする。

【0054】更に、本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムにおける計算機であって、他の計算機におけるユーザから該計算機へのアクセス要求が許可されるべきかどうかを判断し、該計算機への通信がそこからあるユーザによる該計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうかを検査するのに必要なアクセス許可データを生成する管理手段と、該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、を有することを特徴とする計算機を提供する。

【0055】又、本発明は、前記計算機は更に、該計算機へのアクセスが該計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを前記メモリ手段

に記憶した前記アクセス許可データに基づいて判定し、正当と判定された場合、該アクセスを許可する検出手段と、を有することを特徴とする。

【0056】更に、本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを判定し、正当と判定された場合、該アクセスを許可する検出手段と、そこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報と、該あるユーザの該少なくとも一つの計算機における内部ユーザ識別情報との組を記憶するメモリ手段であって、前記検出手段は前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を該メモリ手段が記憶しているとき前記アクセスを正当と判定するものと、前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データが示すユーザ識別情報を該ユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記内部ユーザ識別情報に変換する変換手段と、を有することを特徴とする計算機システムを提供する。

【0057】更に、本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、そこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報と、該あるユーザの該少なくとも一つの計算機における内部ユーザ識別情報との組を示すアクセス許可条件を格納する格納手段と、該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出する検出手段と、該アクセスが間接的になされたものである場合、該アクセスが許可されるべきかどうかを判断し、該アクセスが許可されるべきと判断された場合、該アクセスを許可する管理手段であって、該管理手段は前記他の計算機の発信元システム識別情報を認証し、前記他の計算機の秘密鍵で暗号化された発信元ユーザ識別情報を取得し、該発信元ユーザ識別情報を前記他の計算機の公開鍵を使って復号化することで認証し、認証された発信元ユーザ識別情報と発信元システム識別情報について前記格納手段に格納された前記アクセス許可条件を検査することにより判断するものと、前記検出手段が前記

アクセスを正当と判定したとき、前記アクセスの通信データが示すユーザ識別情報を該ユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記内部ユーザ識別情報に変換する変換手段と、を有することを特徴とする計算機システムを提供する。

【0058】更に、本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムを管理する方法であって、他の計算機におけるユーザから各計算機へのアクセス要求が許可されるべきかどうか判断するステップと、該各計算機への通信がそこからあるユーザによる該各計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成するステップと、該アクセス許可データをメモリに記憶するステップと、該メモリに記憶された該アクセス許可データに基づいて、該各計算機へのアクセスが該各計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを判定し、正当と判定された場合、該アクセスを許可するステップと、を含むことを特徴とする計算機システム管理方法を提供する。

【0059】更に、本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムを管理する方法であって、他の計算機におけるユーザから各計算機へのアクセス要求が許可されるべきかどうか判断するステップと、該各計算機への通信がそこからあるユーザによる該各計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成するステップと、該アクセス許可データをメモリに記憶するステップと、を含むことを特徴とする計算機システム管理方法を提供する。

【0060】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態について説明する。

【0061】（第1の実施の形態）最初に、本発明の各実施の形態において基本となる第1の実施の形態を説明し、次いでいくつかのその応用の実施の形態を説明する。

【0062】まず第1の実施の形態における全体構成を、図1に示す。この図1は、最小構成の場合で、2つの計算機システムから構成されている。

【0063】ユーザ（利用者）が通常利用する計算機システム（ホームシステム）2と、地理的に離れた別の外部の計算機システム（遠隔システム）4がある。通常、このユーザは、ホームシステム2を利用して作業しているが、会議等の場合、出かけていって遠隔システム4を利用する。

【0064】ホームシステム2と遠隔システム4は、各

々の計算機システムに直接接続されたLAN-A8と、LAN-B10を介し、広域ネットワーク6によって接続されている。互いの通信は、標準的なネットワークプロトコルであるTCP/IPで接続されている。ホームシステム2は、ネットワークアドレスAで広域ネットワーク6とつながり、遠隔システム4は、ネットワークアドレスBで広域ネットワーク6と接続されている。

【0065】標準的なネットワークサービスは双方のシステムから利用できる。本実施の形態ではネットワークサービスのうち、RFC959で規定されるリモートファイル転送プログラム(FTP)とRFC854で規定されるリモートログインプログラム(TELNET)を使って説明する。これらのプログラムは、ユーザが起動するクライアントプログラムと、予め起動され、クライアントからのサービス要求を待つサーバプログラムから構成されている(これらのサービスの詳細は、D. Comer著、村井・楠本訳、「TCP/IPによるネットワーク構築 第2版」(共立出版 bit別冊)に詳しい。)

【0066】ホームシステム2と遠隔システム4は、各々所属組織が異なっているので、管理体制は独立しており、ユーザ管理(ユーザIDの登録、削除など)やファイル管理(ファイルごとにファイルのアクセスコントロールを設定し、また、設定されたアクセスコントロールに従ってユーザごとにファイルのアクセスを制限するなど)も計算機システムごとに独立である。

【0067】つまり、図1の構成は、それぞれの計算機の管理が異なった、遠隔システム4とホームシステム2の2台が、広域ネットワーク6を介して接続されている場合である。

【0068】計算機システムの種類については、ホームシステム2と遠隔システム4で計算機システムの種類は同一でも良いし、異なっても良い。例えば、ホームシステム2と遠隔システム4ともにワークステーションシステムである場合、ホームシステム2はメインフレームシステムであり、遠隔システム4はワークステーションシステムである場合などが考えられる。

【0069】本実施の形態の説明では、どちらの計算機システムもUNIXシステム上に構築されているとして説明する。ただし、TCP/IPをサポートしており、FTP、TELNET等のサービスを提供していれば、他のOS上に構築されていても同様である。

【0070】本実施の形態では、計算機システム2, 4の内部機能構成は同一であるとし、これを図2に示す。これが、以下に続く実施の形態の基本構成である。

【0071】図2に示すように、この計算機システム20は、通常の処理100、外部アクセス検出部101、コネクション管理部102、ネットワーク部103、ネットワークデータ加工・復元部104、セッション情報保存部105、セッション情報管理部106、アクセス

許可条件リスト107、署名・認証部108、秘密鍵保存部109、公開鍵取得部110、から構成され、LAN111と接続されている。

【0072】この中で、通常の処理100、コネクション管理部102、ネットワーク部103、LAN111は、従来の計算機、例えば、OSとしてUNIXを載せたワークステーションの機能と変わらない。ユーザ管理は、通常の処理100に含まれる。

【0073】即ち、通常の処理100は、ユーザが直接または間接的に利用する処理全般をいい、通常のWSが持つ機能を指す。具体的機能としては、ログイン処理、ファイルシステム、ユーザ管理部、電子メール、文書エディタ、ワープロ機能、プログラム開発環境、プログラム実行環境、ウィンドウシステムなど、及びネットワークを利用する処理として、リモートログイン、リモートファイル転送などを指す。

【0074】又、コネクション管理部102は、OS17階層モデルでのトランスポート層の処理に相当し、TCP/IPにおいては、TCPやUDPの処理を行う。つまり、1つの計算機システムには、TCPやUDPなどのプロトコル別にポートと呼ばれる識別子があり、このポート単位で、計算機間の通信を行う。

【0075】又、ネットワーク部103は、OS17階層モデルでのネットワーク層の処理に相当し、TCP/IPにおいては、IP処理を行う。複数のデータリンク間をルータで結ぶことによって、計算機システム間の通信が行える。

【0076】これら以外が、本実施の形態において付加された新しい機能に該当するものである。

【0077】即ち、セッション情報管理部106は、遠隔システム4からホームシステム2を利用する場合などに、外部からのアクセスを管理し、外部の正しいユーザからだけと通信できるように管理する部分である。

【0078】又、セッション情報保存部105は、セッション情報管理部106で外部からのアクセスを許可された後述するセッションに関するデータを保存する。このデータは、外部から/外部へのアクセスであるかどうかを外部アクセス検出部101で検出された通信に関し、その通信が許可されたものかどうかを検査するために必要な情報である。又、このデータは、ネットワークデータ加工・復元部104でも用いられる。

【0079】又、アクセス許可条件リスト107は、セッション情報管理部106で利用し、外部から自システムにアクセスしてよい利用可能な諸条件がここに保存される。

【0080】又、署名・認証部108は、外部からアクセスする計算機システムのホストIDやユーザIDに関して、暗号技術を用いて認証を行い、自計算機システムのホストIDやユーザIDに関して、暗号技術を用いて署名を付ける。

【0081】又、公開鍵取得部110は、認証に必要な、外部のマシンまたは、ユーザの公開鍵を検索し、取得する。

【0082】又、秘密鍵保存部109は、署名に必要な、自マシンまたは、自マシン上のユーザの秘密鍵を保管する。

【0083】又、外部アクセス検出部101は、外部からの通信、または、外部への通信を検出し、その通信が、許可された外部のユーザまたは、外部の計算機システムから、または、宛てのものかどうかをセッション情報保存部105に保存された情報を基に、検査する。

【0084】又、ネットワークデータ加工・復元部104は、外部のシステムと通信する際に、通信データの安全のために、データを暗号化したり復号化したりする。また、許可された外部との通信であることを示す認証子をデータに付加したり、外部アクセス検出部101で検査済みのデータから認証子をはずしたりする。

【0085】次に、図3は、複数のホームシステム60が、同一の管理下におかれて1つのホームシステムグループ30として構成されている場合の全体構成である。

【0086】この場合、図3に示すように、機能ごとに複数の計算機に分割して構成してもよい。すなわち、外部ネットワークとの接続点に位置するセキュリティゲートウェイ40、セッション情報管理を担当するセッション情報管理サーバ50、所望の処理を行う複数のホームシステム60からなる構成としてもよい。

【0087】各計算機システムにおける内部機能構成を図4～図6に示す。図中の点線が機能の分割によって各計算機システムにおいて不要になった機能である。

【0088】なお、図3における遠隔システム4の内部機能構成は図1の構成における遠隔システム4の内部機能構成である図2と変わらないので説明は省略する。

【0089】この場合図6に示すホームシステム60は、通常の計算機システムと変わらなくなる。つまり、図3のグループ構成では、通常の計算機システムをホームシステム60として用い、セキュリティゲートウェイ40とセッション情報管理サーバ50を付加することで、図3のシステム構成となる。

【0090】図5に示すセッション情報管理サーバ50は、ホームシステムグループ30内に最低1台あり、ここで、外部との通信に必要なセッションの設立処理を行う。セッション設立が成功した後、必要な情報が、セッション情報保存部105に蓄えられる。この情報は、同時に、セキュリティゲートウェイ40内のセッション情報保存部105へも送られ、蓄えられる。

【0091】図4に示すセキュリティゲートウェイ40は、ホームシステムグループ30と外部とを接続する点に位置する計算機システムであって、ここを通過する通信は、外部アクセス検出部101で検出される。これは、このシステムに入力される通信のパケットのヘッダ

情報をみて、その中の発信元、あて先のネットワークアドレスを検査することで行われる。該当パケットは、セッション情報保存部105のデータと比較され通過できるか判断される。

【0092】外部アクセス検出部101の検査に合格したデータは、ネットワークデータ加工・復元部104で必要な処理が行われたあと通過する。

【0093】セッション設立に必要な通信は、セキュリティゲートウェイ40を通過し、セッション情報管理サーバ50へ送られる。この際の外部からの通信は、セキュリティゲートウェイ40とセッション情報管理サーバ50間に制限されている。

【0094】また、セキュリティゲートウェイ40の内部機能構成においてコネクション管理部102のない構成もある。ネットワーク部103を通る通信のパケットを直接、外部アクセス検出部101にて検査するものである。

【0095】なお、セキュリティゲートウェイ40とセッション情報管理サーバ50は、同一のマシンで構成しても良い。

【0096】また、セキュリティゲートウェイ40の機能をさらに分割し、図7に示すように、外部アクセス検出部101とそれに付随する機能を載せた計算機システム（フィルタリングルータ）70と、図8に示すように、ネットワークデータ加工・復元部104、セッション情報保存部105とそれらに付随する機能を載せた計算機システム（ネットワークデータ処理サーバ）80を別々の計算機システムとして実装してもよい。その場合の全体構成を図9に示す。

【0097】もちろん、それぞれの機能に必要な、セッション情報保存部105は、両方の計算機システムに存在する。この構成の場合、フィルタリングルータ70の機能を、既存のネットワークルータ装置に組み入れることが容易となる。フィルタリングルータ70には、上記のセキュリティゲートウェイ40と同様、コネクション管理部102が存在している構成もある。

【0098】2つの構成を分けた場合、外部からの通信のデータは、フィルタリングルータ70で検査のち、ネットワークデータ処理サーバ80に送られる。また、ホームシステムグループ30内のホームシステム60から外部への通信のデータは、ルータ90を経由してネットワークデータ処理サーバ80へ送られ、そこからフィルタリングルータ70経由で、外部へ送信される（図中の濃い矢印の通信経路）。

【0099】つまり、ホームシステムグループ30内のホームシステム60では、外部あての通信は、一旦、ネットワークデータ処理サーバ80に送られるように、IP層のルーティング情報が設定されている。

【0100】さらに、外部から来た通信のデータは、安全のため、フィルタリングルータ70と、ネットワーク

データ処理サーバ80またはセッション情報管理サーバ50間だけに、IP層における直接の通信が制限されている(図中の淡い矢印が直接通信可能な範囲を示している。))。

【0101】以下、各機能の動作を単純な構成である図2の場合について説明する。ここでの動作は、セッション設立と、セッションを用いた通信との2つの段階に大きく分かれるので、これら各段階を分けて説明する。

【0102】(1)セッション設立

いま、ユーザ田中さんが、ホームシステム2(ネットワークアドレス=A)上にアカウントを持っているものと
10 このユーザ田中さんは、遠隔システム4(ネットワークアドレス=B)にもアカウントを持っており、この遠隔システム4上のユーザIDを101とする。

【0103】遠隔システム4で、ユーザ田中さんが、ホームシステム2にアクセスして、ホームシステム2にログインしたり、ホームシステム2の資源(ファイルなど)をアクセスする際、実際の所望する作業に先立ち、
20 遠隔システム4のセッション情報管理部106とホームシステム2のセッション情報管理部106との間で、ネゴシエーションを行い、アクセス許可を得る。

【0104】この許可の単位のことをセッションと呼ぶことにする。つまり、あるシステムのあるユーザからの通信と、別のあるシステムのあるユーザへの通信が許可された場合、その対をセッションと呼ぶ。

【0105】遠隔システム4では、そのユーザがそのユーザのホームシステム2にアクセスするためのセッションの設立を行い、セッションIDを取得する。以後の実際の所望の通信では、このセッションIDを用いて、
30 ホームシステム2にアクセスすることができ、所望の作業が行える。

【0106】1つのセッションを設立しセッションIDを得るには、以下の動作を行う。ここで、クライアント側(遠隔システム4)のセッション設立時の計算機システムの機能構成を図10に、サーバ側(ホームシステム2)の機能構成を図11にそれぞれ示す。

【0107】I-1. セッション要求データの作成と送信：クライアント側(遠隔システム4)の動作

遠隔システム4のセッション情報管理部106は、遠隔システム4のユーザからの直接的または間接的な指示で、通常の処理100からの指示により、ホームシステム2との間でセッションを設立する。そのため、遠隔システム4のセッション情報管理部106は、ホームシステム2のセッション情報管理部106へセッション設立のための要求データを送信する。

【0108】ここで、本実施の形態におけるセッション設立のために送信するデータ的具体例を示す。

1. 送信元ネットワークアドレス：遠隔システム4のネットワークアドレス(=B)

2. 送信元の計算機システムでのユーザID：遠隔システム4での自分のユーザID(=101)

3. あて先のネットワークアドレス：ホームシステム2のネットワークアドレス(=A)

4. あて先の計算機システムでのユーザID：ホームシステム2での自分のユーザID(=1)

5. 送信元ホストの署名：遠隔システム4の署名データ

6. 送信元ユーザの署名：遠隔システム4のユーザの署名データ

このセッション設立のためのデータのうち、送信元(自システムすなわち遠隔システム4)のネットワークアドレスは、ネットワーク部103で保持しており、ここから指示される。

【0109】自マシンのユーザIDは、セッション設立要求をしたユーザIDのことであり、これは、通常の処理100の中のユーザ管理部(図示せず)で管理されている。このユーザIDが上記の自マシンのデータになる。

【0110】あて先の計算機システム(ホームシステム2)のネットワークアドレスと、そのマシンでのユーザIDは、このセッション設立先の計算機システム(ホームシステム2)のネットワークアドレスと、ユーザIDである。これらは、このセッションを設立しようとするユーザが、直接的または間接的に知らせる。

【0111】ここで、送信元のホストの署名は、以下のようにデータを作成して署名する。即ち、遠隔システム4のネットワークアドレスとホームシステム2のネットワークアドレスとこのデータ作成時の日時の3つのデータを遠隔システム4(自システム)のもつホスト秘密鍵で暗号化したものを送信元ホストの署名データとする。

【0112】又、送信元のユーザの署名は、以下のようにデータを作成して署名する。即ち、遠隔システム4のユーザIDとホームシステム2のユーザIDとこのデータ作成時の日時の3つのデータをユーザ田中さんのもつ秘密鍵で暗号化したものを送信元ユーザの署名データとする。

【0113】本実施の形態では、計算機システムやユーザの署名は、発信元の計算機システム(自システムつまり、遠隔システム4)内の署名・認証部108にて作成する。

【0114】署名に必要な暗号鍵については、自システム(遠隔システム4)のホスト秘密鍵やユーザの秘密鍵を秘密鍵保存部109から得る。ユーザの個人秘密鍵は、ユーザが移動した際に、予め、移動先の秘密鍵保存部109へ入力して保存しておく。

【0115】I-2. セッション要求データの受信とセッションの設立：サーバ側(ホームシステム)の動作
上記I-1のクライアント側の処理について遠隔システム4のセッション情報管理部106で作成されたセッション設立要求データは、コネクション管理部102、ネ
50

ットワーク部103、LAN111、広域ネットワーク6を経て、ホームシステム2に届けられ、更に、ホームシステム2のLAN111、ネットワーク部102、コネクション管理部102を経てホームシステム2のセッション情報管理部106へ届く。

【0116】ここでは、セッション設立要求した、送信元のホストとユーザの認証を行い、今後の実際の所望の作業の処理を実行して良いか判断する。具体的には以下の処理x-1～x-7を行う。

処理x-1 送られてきたデータ中の送信元ホストの送信元ユーザの認証を行う。

処理x-2 図示しない時計などにより、送られたデータが、有効期間内かチェックする。

処理x-3 上記2つの条件に合致したら、図12に示すようなアクセス許可条件リスト107の内容と比較し、要求元のホストやユーザが今後、自システムにアクセスしてよいか判断する。

処理x-4 アクセスが許可されると、新たにセッションを1つ生成し、セッションIDが振られる。

処理x-5 そのセッションに関するセッション情報をセッション情報保存部105に蓄える。その中には、新たに生成され、以後の実際の所望の作業のための通信で必要になるセッション鍵（そのセッションでのみ有効な一時的暗号鍵）が含まれる。

【0117】セッション情報保存部105に蓄えるデータの一例を図13に示す。この図13に示すように、このセッション情報中には、以下に示す内容が含まれる。

1. 自計算機システム（ホームシステム2）でのユーザID
2. 対応する外部計算機システム（遠隔システム4）でのネットワークアドレス
3. 対応する外部計算機システム（遠隔システム4）でのユーザID
4. そのセッションのセッションID
5. そのセッションに有効なセッション鍵
6. 有効期間

【0118】処理x-6 セッション設立に成功すると、セッション要求元である計算機システム（遠隔システム4）にアクセスを許可する旨の回答データを作成して送付する。具体的には、この回答データは以下の内容を含む。

1. 送信元ネットワークアドレス：ホームシステム2のネットワークアドレス（＝A）
2. 送信元の計算機システムでのユーザID：ホームシステム2での自分のユーザID（＝1）
3. あて先のネットワークアドレス：遠隔システム4のネットワークアドレス（＝B）
4. あて先の計算機システムでのユーザID：遠隔システム4での自分のユーザID（＝101）
5. 送信元ホストの署名：ホームシステム2の署名デー

タ

6. 送信元ユーザの署名：ホームシステム2のユーザの署名データ

7. セッションID：そのセッションを識別するID

8. セッション鍵：そのセッションで有効な一時的暗号鍵

9. 有効期間：そのセッションの有効な期間

【0119】ここで、送信元を特定するため（偽のホームシステムでないことを検査するため）に、送信元のホスト名とユーザ名の署名を付ける。署名の付け方は、上述したセッション設立要求時の署名作成の処理と同様である。

【0120】同時に返送する、セッション鍵も別のホストで解読されないように、以下の処理を行って送られる。即ち、セッション鍵をあて先のホスト（遠隔システム4）の公開鍵と送信元のホスト（ホームシステム2）の秘密鍵で暗号化してから送付する。

【0121】処理x-7 アクセス許可条件に適合せず、セッション設立に失敗すると、その旨のデータを送信元である計算機システム（遠隔システム4）に返す。

【0122】ここで、上記の処理x-1の認証処理を更に詳しく説明する。送られてきたデータのうち、送信元ホスト（遠隔システム4）の認証は、ホスト認証のための署名データを用い、このデータを遠隔システム4の公開鍵を用いて復号化する。

【0123】復号化された平文中に書かれている送信元ホストアドレスとあて先ホストアドレスがそれぞれ、遠隔システム4とホームシステム2のアドレスに一致し、かつ、日時データが本認証処理を行っている時間と、予め定めてある期間以内であれば、認証成功と判断する。

【0124】送信元ホストのユーザの認証は、送られたデータ中のユーザ認証のためのデータを用いる。あて先ユーザIDのデータから、自システム（ホームシステム2）のユーザIDに該当するユーザ名を通常の処理100の中に含まれるユーザ管理部（図示せず）から求め、そのユーザ名に対応する公開鍵を公開鍵取得部110から得て、これを用い復号化する。

【0125】復号化された平文中に書かれている送信元（遠隔システム4）のユーザIDとあて先（ホームシステム2）のユーザIDが、要求データ中の各々に一致し、かつ、日時データが、本認証処理を行っている時間と、予め定めてある期間以内であれば、認証成功と判断する。

【0126】この認証処理で使う遠隔システム4の公開鍵とユーザの公開鍵は、公開鍵取得部110より得る。ここに該当する公開鍵が保存されていなければ、ここからネットワーク部103を経て外部の公開鍵サーバ（図示せず）より入手する。

【0127】I-3. Nセッション要求の回答データの受信：クライアント側（遠隔システム4）の動作

遠隔システム4では、ホームシステム2からセッション設立の要求に対する回答データを受けると、遠隔システム4のセッション情報管理部106が、受け取ったデータからセッション情報保存部105にデータを保存する。

【0128】ここでセッション情報保存部105に保存されるデータは、具体的には、以下のデータを含む。

1. 自計算機システム（遠隔システム4）でのユーザID
2. 対応する外部計算機システム（ホームシステム2）のネットワークアドレス
3. 対応する外部計算機システム（ホームシステム2）でのユーザID
4. そのセッションのセッションID
5. そのセッションに有効なセッション鍵
6. 有効期間

【0129】受信したデータ中のホスト署名とユーザ署名を検査し、セッション設立要求先のホストからの正当な回答であることを確認する。署名の認証方法は、上記処理x-1の場合と同様である。

【0130】また、セッション鍵は暗号化されているので、自ホストの秘密鍵と相手ホストの公開鍵を用いて、上記処理x-1と同様の方法で復号して元通りのセッション鍵を得る。

【0131】(II) セッションを用いた通信
セッション設立処理が終了すると、所望の処理が開始できる。ここでは各計算機システムが図14の機能構成となり、クライアント側の処理と、サーバ側の処理が以下のように行われる。

II-1. クライアント側の動作

II-1-1: 送信

許可された外部の計算機システム（遠隔システム4）が、ホームシステム2にデータを送信する。送信データは、通常の処理100の部分で作成され、特別な処理を行わずに送信され、外部アクセス検出部101へ送られる。

【0132】外部アクセス検出部101ではデータのあて先を検出する。コネクション管理部102がTCPの処理を行っているとなると、各通信コネクションごとに通信相手のホストのネットワークアドレスやTCPのポート番号などを管理しているので、ここから必要な情報が得られる。外部アクセス検出部101は、この情報をセッション情報保存部105のデータと比較してことを通過するデータが外部あてのデータかどうか判断する。

【0133】外部あてのデータであると、これがネットワークデータ加工・復元部104に送られ、データの加工が行われる。内部あてであると、そのまま素通りし、通常の通信どおり、コネクション管理部102、ネットワーク部103を通り、LAN111を経て、あて先へ送信される。

【0134】ネットワークデータ加工・復元部104に送られたデータは、必要な処理が施される。一例としては、このデータのあて先（ホームシステム2）に対して、許可された外部ホストからのデータであることを示すためにMAC（Message Authentication Code）をセッションIDと共に付加する。このMACを得るには、あて先ごとに保存されているセッション情報保存部105のセッション鍵を用いる。これを用いて、送信データのハッシュ値を計算し、MAC値とする。ハッシュ値の計算方法は、RFC1321で規定されるMD5による。

【0135】さらに、送信するデータの重要度や途中の通信経路によっては、データの盗聴防止のため、暗号化処理が必要になる。その場合には、MACを生成する時に利用した同じセッション鍵を用いてたとえばDES方式でデータ自身を暗号化する。

【0136】いずれの場合も、送信するデータに加工したので、それに伴って送信データのフォーマットの変更も必要に応じて行う。

【0137】ネットワークデータ加工・復元部104で加工された外部あてのデータは、再び外部アクセス検出部101に戻り、コネクション部102、ネットワーク部103、LAN111を経て、外部ネットワーク6経由であて先であるホームシステム2へ送られる。

【0138】なお、上記の処理では、外部あてのデータを外部アクセス検出部101においてセッション情報保存部105のデータと比較して検出していたが、外部あてのデータの検出は、簡略して次のようにして行っても良い。

【0139】つまりホームシステムグループにて利用している範囲のネットワークアドレスを予め、外部アクセス検出部101内に保存し、それを使って、通信のデータのあて先を外部あてのものかどうか判断してもよい。

【0140】外部あてと判断されたデータは、ネットワークデータ加工・復元部104に送られ、ここで、セッション情報保存部105のデータと比較し、真に外部へアクセス許可された通信のデータか判断し、MACの付加等の処理を行う。

【0141】II-1-2: 受信

外部ホスト（ホームシステム2）からの受信データは、LAN111、ネットワーク部103、コネクション管理部102と通って、外部アクセス検出部101に届く。ここで、外部からの通信かどうか検出され、外部からアクセス可能な通信か検査される。この判断に必要な情報は、セッション情報保存部105から得られる。

【0142】内部からのデータであると、そのまま外部アクセス検出部101を素通りし、通常の処理100へ渡される。

【0143】外部からのアクセスの場合、さらに、ネットワークデータ加工・復元部104に送られ、必要に

じてデータの復元がなされる。復元に必要な情報は、セッション情報保存部105から得られる。そして、復元後、外部アクセス検出部101を経て、自システム内の通常の処理100に引き渡される。

【0144】詳細に説明すると、コネクション管理部102を通ったデータは、外部アクセス検出部101で、データの発信元を検査される。コネクション管理部102がTCPの処理を行っているとする、各通信コネクションごとに通信相手のホストのネットワークアドレスやTCPのポート番号などを管理しているので、ここから必要な情報が得られる。つまり、IPパケットのヘッダ情報の中からあて先と送信元のIPアドレス、TCPのヘッダ情報からあて先と送信元のポート番号が得られる。この情報を、セッション情報保存部105のデータと比較し、外部からのアクセスかどうか判断する。

【0145】また、データ中にMACが入っている時は、このMACを用いて外部からアクセス可能な通信か検査できる。MACを生成した処理と同様に、このデータ中からセッションIDを得、それに対応したセッション鍵をセッション情報保存部105から得、そのセッション鍵を利用して、MACを生成したのと同じ手順で計算する。計算結果がデータ中に書かれているMACの値と一致するか検査し、正しいアクセスか判断する。

【0146】II-2：サーバ側の処理

サーバ側の処理も上述したクライアント側と同様である。ただし、ネットワークデータ加工・復元部104の処理において、さらに、外部から受け取ったデータのセッションIDを用いて、データ中に記述されているユーザIDを遠隔システム4のユーザIDからホームシステム2のユーザIDに変換したり、外部へ送るデータ中のホームシステム2のユーザIDを遠隔システム4のユーザIDに変換したりする、ユーザID変換処理を合わせて行うこともできる。

【0147】その結果、通常の処理100において、ホームシステム2の該当ユーザIDのアクセス権限で、リモートファイル転送によるファイルシステムに対するコピーなどのファイル操作やリモートログインなどのアクセスが可能になる。

【0148】(第2の実施の形態)次に、本発明の第2の実施の形態について説明する。この第2の実施の形態の全体構成は、上述した図1と同様である。

【0149】ユーザ(利用者)が通常利用する計算機システムと(ホームシステム)2と、地理的に離れた別の外部の計算機システム(遠隔システム)4がある。通常、このユーザは、ホームシステム2を利用して作業しているが、会議等の場合、出かけて行って遠隔システム4を利用する。

【0150】ホームシステム2と遠隔システム4は、各々の計算機システムに直接接続されたLAN-A8と、LAN-B10を広域ネットワーク6によって接続され

ている。互いの通信は、標準的なネットワークプロトコルであるTCP/IPで接続されている。ホームシステム2は、ネットワークアドレスAで広域ネットワーク6とつながり、遠隔システム4は、ネットワークアドレスBで広域ネットワーク6と接続されている。

【0151】標準的なネットワークサービスは双方のシステムから利用できる。本実施の形態ではネットワークサービスのうち、リモートファイル転送プログラム(FTP)とリモートログインプログラム(TELNET)を使って説明する。これらのプログラムは、ユーザが起動するクライアントプログラムと、予め起動され、クライアントからのサービス要求を待つサーバプログラムから構成されている。

【0152】ホームシステム2と遠隔システム4は、各々所属組織が異なっているので、管理体制は独立しており、ユーザ管理(ユーザIDの登録、削除など)やファイル管理(ファイルごとにファイルのアクセスコントロールを設定し、また、設定されたアクセスコントロールに従ってユーザごとにファイルのアクセスを制限するなど)も計算機システムごとに独立である。

【0153】計算機システムの種類については、ホームシステム2と遠隔システム4で計算機システムの種類は同一でも良いし、異なっても良い。例えば、ホームシステム2と遠隔システム4ともにワークステーションシステムである場合、ホームシステム2はメインフレームシステムであり、遠隔システム4はワークステーションシステムである場合などが考えられる。

【0154】本実施の形態の説明では、どちらの計算機システムもUNIXシステム上に構築されているとして説明する。ただし、TCP/IPをサポートしており、FTP、TELNET等のサービスを提供していれば、他のOS上に構築されていても同様である。

【0155】本実施の形態では、計算機システム2、4の内部機能構成は同一であるとし、これを図15に示す。図15に示すように、この計算機システム150は、入出力部201、ローカルログイン202、外部アクセス検出部101、アクセス許可条件リスト107、ユーザ管理部203、個人スケジュール管理部151、リモートログイン204、リモートファイル転送206、ファイルシステム205、ユーザID共通化部106A、ユーザID対応管理表105A、コネクション管理部102、ネットワーク部103、一時的パスワード入力152、一時的パスワード生成153から構成される。

【0156】上記第1の実施の形態との比較では、通常の処理100と対応するものは、入出力部201、ローカルログイン202、リモートログイン204、ユーザ管理部203、リモートファイル転送206、ファイルシステム205である。図2のセッション情報管理部106には、ユーザID共通化部106Aが対応し、図2

のセッション情報保存部105とは、ユーザID対応管理表105Aが対応する。また、図2のネットワークデータ加工・復元部104に相当するところは存在せず、図2の署名・認証部108、公開鍵取得部110、秘密鍵保存部109に対応するものもなく、代わりに、個人スケジュール管理部151と一時的パスワード入力152と一時的パスワード生成153が新たに付加されている。

【0157】ここで入出力部201は、ユーザが計算機システム2、4を直接使用するための入力装置及び出力装置から構成される。入力装置としては、キーボード、マウス、さらには、シリアル回線等を利用することができる。出力装置としては、ディスプレイ、プリンタ、さらには、シリアル回線などを利用することができる。入出力部201は、ローカルログイン202を介して、内部の構成部分に接続される。

【0158】次に、この第2の実施の形態における動作を説明する。いま、あるユーザ田中さんが、ホームシステム2上にアカウントをもっているものとする。そのホームシステム2上でのユーザIDを1とする。このユーザ田中さんは、遠隔システム4にもアカウントを持っており、その遠隔システム4上のユーザIDを101とする。

【0159】ホームシステム2上には、個人スケジュール管理部151が稼働していて、個人ごとのスケジュールを管理している。ここで用いるスケジュール管理表の例を図16に示す。個人スケジュール管理部151は図16のように、ユーザごとにスケジュールの内容を書いた表をもっている。例では、田中さん（ユーザID=1）は、「本日午後遠隔システムへ行って、作業をする」ことになっている。

【0160】外出する際に、田中さんは、ホームシステム内の一時的パスワード生成153に、出先の計算機システム（遠隔システム4）から当該ホームシステム2を使用するために必要な一時的パスワードを発行してもらう。

【0161】一時的パスワード生成153は、以下に示す処理a-1～処理a-6を行って、一時的パスワードを発行する。

処理a-1 要求ユーザのユーザIDを得る。

処理a-2 そのユーザIDのスケジュールデータを個人スケジュール管理部151から得る。

処理a-3 外出先のネットワークアドレスと外出期間をスケジュール管理表から得る。

処理a-4 その外出先を識別するための一時的なパスワード（第1の実施の形態におけるセッションIDに相当）の生成と、有効期間の計算をする。

処理a-5 アクセス許可条件リスト107に、図17のように、「ユーザID」、「外出先ネットワークアドレス」、「一時的パスワード」、「有効期間」、「その

他の情報（ファイル読みだしのみ許可などその他の許可条件など）」を登録する。

処理a-6 要求ユーザに一時的パスワードを返す。

【0162】次に、ユーザ田中さんの外出先の遠隔システム4での動作を説明する。ユーザ田中さんは、外出先に行き、そこにある遠隔システム4を使用して作業を行う。ユーザ田中さんは、遠隔システム4上のユーザアカウントを作成し、または以前作成して使っていたユーザIDを利用して、所望の作業を行う。ユーザ田中さんのユーザIDは101とする。ユーザ田中さんが、遠隔システム4からホームシステム2にアクセスする際には、予め、遠隔システム4で作業するユーザ田中さんからの起動により、遠隔システム4のユーザID共通化部106Aで、図18に示すような、上記セッション設立に相当するユーザID共通化のためのユーザID共通化要求のデータを作成し、ホームシステム2のユーザID共通化部106Aとコネクションを張り、ユーザのIDの共通化作業を行う。

【0163】ここで、本実施の形態におけるユーザID共通化の要求のためのデータの具体例を示す。

1. 送信元ネットワークアドレス：遠隔システム4のネットワークアドレス（=B）
2. 送信元の計算機システムでのユーザID：遠隔システム4での自分のユーザID（=101）
3. あて先のネットワークアドレス：ホームシステム2のネットワークアドレス（=A）
4. あて先の計算機システムでのユーザID：ホームシステム2での自分のユーザID（=1）
5. あて先の一時的パスワード生成153から得た一時的パスワード

【0164】上記のユーザID共通化の要求のためのデータのうち、送信元（自システム即ち遠隔システム4）のネットワークアドレスとユーザIDは、自動的に作成される。つまり、自ネットワークアドレスは、ネットワーク部103で保持しており、ユーザIDは、ユーザ管理部203で保持している。

【0165】あて先の計算機システム（ホームシステム2）の一時的パスワード生成153から発行された一時的パスワードは、ユーザから入力させて一時的パスワード入力152に情報を得る。

【0166】次に、遠隔システム4からユーザID共通化の要求のためのデータが送られてきたホームシステム2側では、ユーザID共通化部106Aにて、以下の処理b-1～処理b-5の手順でユーザID共通化の判断と登録を行う。処理b-1 送られてきたデータが図7のアクセス許可条件リスト107の内容と合致するか検査する。処理b-2 図示しない時計などにより、現在が有効期間内かチェックする。処理b-3 そのほかの条件があれば、それに適合するか検査する。処理b-4 上記3の条件に合致したら、図19に示すようにユーザI

D対応管理表105Aにアクセス許可データを登録し、送信元である計算機システム（遠隔システム4）にアクセスを許可する旨を通知する。

【0167】なお、アクセス許可データとしての登録内容を以下に示す。

1. 自計算機システム（ホームシステム2）でのユーザID
2. 対応する外部計算機システム（遠隔システム4）のネットワークアドレス
3. 対応する外部計算機システム（遠隔システム4）でのユーザID
4. 有効期間
5. その他の情報

処理b-5 上記3つの条件に合致しなければ、その旨のデータを発信元である計算機システム（遠隔システム4）に返す。

【0168】以後、許可された外部の計算機システム（遠隔システム4）のユーザIDからの所望の処理に伴う指示に従い、上記のユーザID対応管理表105Aに従った自計算機システム（ホームシステム2）に該当するユーザIDのアクセス権限でアクセスされる。例えば、リモートファイル転送によるファイルシステムに対するコピーなどのファイル操作やリモートログインなどのアクセスが可能になる。

【0169】たとえば、ユーザ田中さんは、遠隔システム4を利用して、ホームシステム2のファイルをコピーしたいとき、リモートファイル転送プログラムを利用する。この時の手順は、以下のような処理c-1～処理c-12となる。なお、この手順にて交換される情報の流れを、図20に示す。

【0170】処理c-1 ユーザ田中さんは、遠隔システム4のリモートファイル転送206（クライアント側）をユーザID=101の権限として起動させる。

【0171】処理c-2 そのプログラムは、外部アクセス検出部101、コネクション管理部102、ネットワーク部103、LAN111を経て相手計算機システム（ホームシステム2）と通信路を設定し（IPデータグラム通信が可能になる）、TCPのコネクション設定を要求する。本実施の形態では、クライアント側の外部アクセス検出部101は、素通りで動作しない。

【0172】処理c-3 相手計算機システム（ホームシステム2）のネットワーク部103を通り、コネクション管理部102へ要求がくる。

【0173】処理c-4 相手計算機システム（ホームシステム2）のコネクション管理部102では、発信元計算機システム（遠隔システム4）とのTCPのコネクションを張り、外部アクセス検出部101を通り、リモートファイル転送206（サーバ側）を起動しようとする。

【0174】処理c-5 ホームシステム2の外部ア

セス検出部101は、上記のコネクション要求を検出し、接続の可否の判断処理を開始する。つまり、コネクション管理部102へ、発信元計算機システム（遠隔システム4）のネットワークアドレスとユーザIDを要求する。

【0175】処理c-6 上記コネクション管理部102では、ネットワークのコネクションを張る段階で発信元計算機システム（遠隔システム4）のネットワークアドレスやコネクション識別子（ポート番号）が得られている。これは、TCPのプロトコルの仕様に基づくものである。

【0176】処理c-7 更に、発信元計算機システム（遠隔システム4）のコネクション管理部102に付随する図示しないユーザ・コネクション対応管理部に問い合わせることにより、このコネクションを張った発信元計算機システム（遠隔システム4）のユーザIDなどの情報が得られる。ユーザIDとコネクションの対応は、identificationプロトコル（RFC1413などで規定）に従って決められているものである。

【0177】処理c-8 受信側計算機システム（ホームシステム2）のコネクション管理部102は、上記2つのデータ（発信元ネットワークアドレスとユーザID）を要求元計算機システム（遠隔システム4）の外部アクセス検出部101に伝える。

【0178】処理c-9 受信側計算機システム（ホームシステム2）の外部アクセス検出部101は、これらのデータをセッション情報保存部105のデータと比較して合っているか検査し、このコネクションをリモートファイル転送206（サーバ側）につなげるかの判断をする。

【0179】処理c-10 検査に合格すると、外部アクセス検出部101では、外部の計算機システム（遠隔システム4）との間のコネクションをリモートファイル転送206（サーバ側）につなぎ、実際のファイル転送の処理を開始できる状態にする。

【0180】処理c-11 検査に合格しないと発信元計算機システム（遠隔システム4）に不許可の返事を返し、コネクションの切断をコネクション管理部102へ指示する。

【0181】処理c-12 合格した場合、リモートファイル転送が遠隔システム4のユーザに対し利用可能になり、遠隔システム4側のリモートファイル転送206（クライアント側）は、通常の処理を開始する。つまり、ログイン処理を行い、遠隔システム4のユーザに、ホームシステム2のユーザIDとパスワードを要求し、ログインに成功すると、実際のファイル転送の処理を行う。

【0182】リモートログイン処理の場合も同様に、外部の計算機システム（遠隔システム4）のネットワークアドレスとユーザIDでアクセス許可の判定を行ってか

ら、実際の処理をはじめることができる。

【0183】以上説明したように、本実施の形態によれば、管理や計算機システムの構成の異なる複数の計算機システムをネットワークを介して接続した分散環境において、各計算機システムでユーザ管理やファイル管理が異なるのにも関わらず、ユーザが移動した先の計算機システムにおいて安全にファイルなどの個人情報を扱えるので、地理的に分散した環境下でも効率よい個人作業支援が可能になる。

【0184】すなわち、本実施の形態では、予め、ユーザIDごとのスケジュール管理表に移動先に計算機システムを特定する情報、例えばネットワークアドレスを記入してから移動し、移動先の計算機システムからリモートアクセスするので、そこに記入された移動先からしかリモートアクセスできず、セキュリティが強化される。さらに移動先に予めわかっているので、移動先で必要になるファイルの先送りが可能になる。また、電子メールの到着を移動先に回送することも可能になり、移動先でのユーザの利便は著しく向上する。

【0185】又、移動先のユーザIDと移動元のユーザIDが同一ユーザであるかどうかの判断は、計算機システムにログインするためのパスワードでなく、その時の移動に関する一時的なパスワードであるので、パスワードの盗聴によるパスワードの漏洩の危険が著しく低下される。

【0186】本実施の形態では、計算機システムやユーザの識別のために、ネットワークアドレスやユーザID Eを利用したが、別の識別名、例えばネットワークアドレスの代わりにシステムID、ホスト名、ドメイン名などを利用し、ユーザIDの代わりにユーザ名、電子メールアドレスのようなユーザ名とドメイン名を組にしたものなどを利用しても良い。

【0187】尚、本実施の形態では、外出先の遠隔システム4とホームシステム2間で、ユーザID共通化処理を行う際、要求データの中に、一時的パスワードをそのままいれて、ホームシステム2に送っていたが、上記第1の実施の形態のように、この一時的パスワードを暗号鍵として用い、遠隔システム4からパスワードそのものを送るのではなく、ユーザ名や、遠隔ホスト名、日時データなどをその鍵で暗号化して送り、受け手のホームシステム2では、そのユーザに対応する一時的パスワードを暗号鍵として復号化して検査することも可能である。

【0188】(第3の実施の形態) 次に、本発明の第3の実施の形態について説明する。この第3の実施の形態の全体構成は、上述した図1と同様である。

【0189】本実施の形態では、計算機システム2、4の内部機能構成は同一であるとし、これを図21に示す。図21に示すように、この計算機システム210は、入出力部201、ローカルログイン202、外部アクセス検出部101、ユーザ管理部203、リモートロ

グイン204、リモートファイル転送206、ファイルシステム205、ユーザID共通化部106A、コネクション管理部102、ネットワーク部103、個人情報鍵入力部213、署名・認証部108、公開鍵取得部110、秘密鍵保存部109、計算機システム秘密鍵保存部212、ユーザID対応管理表105Aから構成される。

【0190】上記第1の実施の形態との比較では、通常の処理100と対応するものは、入出力部201、ローカルログイン202、リモートログイン204、ユーザ管理部203、リモートファイル転送206、ファイルシステム205である。図2のセッション情報管理部106には、ユーザID共通化部106Aが対応し、図2のセッション情報保存部105とは、ユーザID対応管理表105Aが対応する。又、図2のアクセス許可リスト107とネットワークデータ加工・復元部104に相当するところは存在せず、秘密鍵保存部109に、個人情報鍵入力部213と計算機システム秘密鍵保存部212が付加されている。

【0191】次に、この第3の実施の形態における動作を説明する。

【0192】両システム2、4をつなぐ、ネットワークプロトコルは、上記第1、第2の実施の形態と同様TCP/IPとする。従って、ネットワーク部103はIP処理を行い、コネクション管理部102はTCPの処理を行う。また、TELNET、FTP等のサービスも実行できるものとする。

【0193】いま、ユーザ田中さんが、ホームシステム2上にアカウントを持っているものとする。そのホームシステム2上でのユーザIDを1とする。このユーザ田中さんは、遠隔システム4にもアカウントを持っており、その遠隔システム4上のユーザIDを101とする。

【0194】まず、本実施の形態における認証方式について説明する。認証は、個人と計算機システムの両方で可能であり、公開鍵暗号方式で認証を行うことができる。つまり、ユーザ個人や計算機システムは、自己固有の秘密鍵をもっている。この秘密鍵は、非公開で、計算機システムやユーザ自己で安全に管理する。計算機システムの秘密鍵は、計算機システム秘密鍵保存部212に安全に保存されている。これは、OSのカーネル内など、そのシステムで安全な部分に保存されている。ユーザ個人の秘密鍵は、他人には知られない形かつユーザ本人が必要な時に移動先でも使えるように、ICカードや、磁気カードなどに記憶させておくのが好ましい。

【0195】この秘密鍵とペアになる公開鍵は、公開鍵サーバ等に登録し、各計算機システム内の公開鍵取得部110で自由に検索して取得できる。

【0196】従って、各ユーザは、ユーザ固有の秘密鍵を安全な形で持って外部に出向き、外部の利用先からそ

の個人の秘密鍵を用いてアクセスする。

【0197】よって、ユーザ田中さんは、田中さん個人しか知らない秘密鍵をもっている。これを、本実施の形態では、公開鍵暗号方式で実現する。

【0198】次に、ユーザ田中さんの外出先の遠隔システム4での動作を説明する。ユーザ田中さんは、外出先いき、そこにある遠隔システム4を使用して作業を行う。ユーザ田中さんは、遠隔システム4上のユーザアカウントを作成し、または、以前作成して使っていたユーザIDを利用して、所望の作業を行う。ユーザ田中さんのユーザIDは101とする。ユーザ田中さんが、遠隔システム4からホームシステム2にアクセスする際には、予め、遠隔システム4で作業するユーザ田中さんからの起動により、遠隔システム4のユーザID共通化部106Aで、図22に示すような、上記セッション設立に相当するユーザID共通化のためのユーザID共通化要求のデータを作成し、ホームシステム2のユーザID共通化部106Aとコネクションを張り、ユーザIDの共通化作業を行う。

【0199】ここで、本実施の形態におけるユーザID共通化の要求のためのデータの具体例を示す。

1. 送信元ネットワークアドレス：遠隔システム4のネットワークアドレス(=B)
2. あて先のネットワークアドレス：ホームシステム2のネットワークアドレス(=A)
3. 計算機システムの認証のための署名：遠隔システム4のネットワークアドレスとホームシステム2のネットワークアドレスを遠隔システム4のもつ秘密鍵とホームシステム2の公開鍵を暗号化したもの
4. 送信元の計算機システムでのユーザID：遠隔システム4での自分のユーザID(=101)
5. あて先の計算機システムでのユーザID：ホームシステム2での自分のユーザID(=1)
6. ユーザIDの認証のための署名：遠隔システム4のユーザIDとホームシステム2のユーザIDを田中さんのもつ秘密鍵で暗号化したもの

【0200】上記のユーザID共通化の要求のためのデータのうち、送信元(自システムすなわち遠隔システム4)のネットワークアドレスとユーザIDは、自動的に作成される。つまり、自ネットワークアドレスは、ネットワーク部103で保持しており、ユーザIDは、ユーザ管理部203で保持している。

【0201】共通化を行う相手(あて先すなわちホームシステム2)のネットワークアドレスとユーザIDは、ユーザから情報を得る。

【0202】本実施の形態では、計算機システムの認証のための署名は、署名・認証部108にて作成する。あて先のシステム(ホームシステム2)のネットワークアドレスと発信元システム(遠隔システム4)のネットワークアドレス(すなわち自システムのネットワークアド

レス)はすでに得られているので、これらに加えて、新たにあて先の計算機システム(ホームシステム2)の公開鍵を公開鍵取得部110より入手し、自システム(遠隔システム4)の秘密鍵を秘密鍵保存部109から得る。ここには、計算機システム秘密鍵保存部212から得られた鍵が保管されている。これらから、あて先の計算機システム(ホームシステム2)のネットワークアドレスと発信元計算機システム(遠隔システム4)のネットワークアドレスを発信元の計算機システムの秘密鍵とあて先計算機システム(ホームシステム2)の公開鍵で暗号化してシステム認証のための署名が作成される。

【0203】ユーザIDの認証のための署名の作成も、署名・認証部108にて同様に行う。ユーザの個人秘密鍵は、秘密鍵保存部109から得る。ここへは、ユーザが個人秘密鍵入力部213に入力することでユーザの個人秘密鍵が得られている。あて先計算機システム(ホームシステム2)上のユーザIDと自システム(遠隔システム4)のユーザIDは既に得られているので、この2つを個人秘密鍵で暗号化することで署名ができる。

【0204】次に、遠隔システム4からユーザID共通化の要求のためのデータが送られてきたホームシステム2側では、ユーザID共通化部106Aにて、以下の処理d-1～処理d-4の手順でユーザID共通化の判断と登録を行う。処理d-1 送られてきたデータ利用して、発信元計算機システム(遠隔システム4)のIDを認証する。処理d-2 さらに、送られてきたデータを利用して、発信元ユーザの認証をする。処理d-3 上記2つの認証が成功したら、(上記第1の実施の形態におけるアクセス許可条件リストに相当するものがないので)、アクセスが許可されたとし、図19に示すようにユーザID対応管理表105Aにアクセス許可データを登録し、送信元である計算機システム(遠隔システム4)にアクセスを許可する旨を通知する。

【0205】なお、アクセス許可データとしての登録内容を以下に示す。

1. 自計算機システム(ホームシステム2)でのユーザID
2. 対応する外部計算機システム(遠隔システム4)のネットワークアドレス
3. 対応する外部計算機システム(遠隔システム4)でのユーザID
4. 有効期間

処理d-4 認証が成功しなければその旨のデータを発信元である計算機システム(遠隔システム4)に返す。

【0206】次に上記の処理d-1の認証処理をさらに詳しく説明する。送られてきたデータのうちシステム認証のための署名から、ホームシステム2の秘密鍵と遠隔システム4の公開鍵を用いて署名・認証部108にて認証を行う。

【0207】ホームシステム2の秘密鍵は、秘密鍵保存

部109から得られ、ここには、計算機システム秘密鍵保存部212から得られた鍵が保管されている。遠隔システム4の公開鍵は、公開鍵取得部110より得る。ここに該当する公開鍵を保存していなければ、ここからネットワーク部103を経て外部の公開鍵サーバ（図示せず）より入手する。この2つの鍵を使って上記の署名を復号し、平文を得る。平文が、確かにホームシステム2のネットワークアドレスと遠隔システム4のネットワークアドレスとに一致したときに、認証が成功する。

【0208】次に、処理d-2の認証処理をさらに詳しく説明する。処理d-1と同様に、送られてきたデータのうちユーザ認証のための署名を、該当ユーザの公開鍵を使って復号し、平文を得る。この平文が、同時に送られてきたデータ中の送信元のあて先の計算機システムのユーザIDと一致するか否かの検査を行い、一致したときに認証が成功する。なお、公開鍵は、公開鍵取得部110により得る。

【0209】上記の処理d-3は、第2の実施の形態における処理b-4と同様である。ただし、本実施例の形態では第2の実施の形態の個人スケジュール管理を省いているので、有効期間を一律現在時から例えば4時間と設定する。

【0210】第2の実施の形態のように、ユーザごとにスケジュール管理表、または、別の指示によって、アクセス許可条件リストを作成し、この表を用いて外部からのホストやユーザなどのアクセス先とアクセス時間を制限してもよい。また、ユーザIDの代わりにユーザ名などを用いてもよい。

【0211】尚、本実施の形態では、システムの認証にネットワークアドレスまたはシステム名を用いるが、地理的場所（住所）によるアクセス制限も可能である。この場合、別の手段で提供される地理的場所と、これとネットワークアドレスまたはシステム名との対応関係を保持する手段とを組み合わせることで実現できる。これはたとえば、ネットワーク管理システムで保持しているデータベースからの情報提供を受けることで可能となる。このデータベースは、図23のようにネットワークアドレス、ホスト名、設置場所の関係を管理しており、ネットワークトラブルや、トラフィックス監視などのネットワーク管理業務に利用している。このデータベースを利用すると、「関東地区からの外部アクセス可」とか、「本社会議室のみアクセス可」などの制限が可能になる。この場合、個人スケジュール表にかえて、外部アクセス許可表をユーザごとに作成し、ユーザID共通化において、認証が成功した後、このアクセス許可表に記載された内容（許可時間と場所）なら外部アクセスを許可する方式となる。

【0212】（第4の実施の形態）次に、本発明の第4の実施の形態について説明する。上記第2および第3の実施の形態では、遠隔システム4へ移動したユーザが、

ホームシステム2との間でユーザID共通化を行ったのち、実際の作業をはじめる方式を用いたが、この第4の実施の形態は、ユーザが所望する作業を直接行う方式を用いる。この第3の実施の形態の全体構成は、上述した図1と同様である。

【0213】本実施の形態では、計算機システム2、4の内部機能構成は同一であるとし、これを図24に示す。図24に示すように、この計算機システム240は、入出力部201、ローカルログイン202、ユーザ管理部203、リモートログイン204、リモートファイル転送206、ファイルシステム205、コネクション管理部102、ネットワーク部103、署名・認証部108、公開鍵取得部110、計算機システム秘密鍵保存部212、秘密鍵保存部109、ユーザ・コネクション対応管理部211、ユーザID変換部104A、外部アクセス許可判断部106B、外部アクセス検出部101、アクセス許可条件リスト107から構成される。

【0214】上記第1の実施の形態との比較では、通常の処理100と対応するものは、入出力部201、ローカルログイン202、ユーザ管理部203、リモートログイン204、リモートファイル転送206、ファイルシステム205である。但し、リモートログイン204とリモートファイル転送206は、ユーザID変換部104Aから指示されたユーザIDの権限で直接起動され、各プログラムの中で再度ユーザIDの入力処理をしないように、改造されているものである。図2のネットワークデータ加工・復元部104とは、ユーザID変換部104Aが対応し、秘密鍵保存部109に、計算機システム秘密鍵保存部212が付加されている。又、図2のセッション情報管理部106とは、外部アクセス許可判断部106Bが相当するが、セッション情報保存部105と相当するところはない。又、コネクション管理部102には、ユーザ・コネクション対応管理部211が付加されている。

【0215】両システム2、4をつなぐネットワークプロトコルは、第1～第3の実施の形態と同様、TCP/IPとする。従って、ネットワーク部103はIP処理を行い、コネクション管理部102はTCPの処理を行う。また、TELNET、FTP等のサービスも実行できるものとする。

【0216】本実施の形態においても、第3の実施の形態と同様なシステム間の認証機能を有し、所望の処理に先だって、計算機システム間の認証処理を行うが、これは上記第3の実施の形態と同様であるので、ここでの説明は省略する。

【0217】いま、ユーザ田中さんが、ホームシステム2上にアカウントを持っているものとする。そのホームシステム2上でのユーザIDを1とする。このユーザ田中さんは、遠隔システム4にもアカウントを持っており、その遠隔システム4上のユーザIDを101とす

る。これら両ユーザIDの対応関係は、予め、両システム2、4間で取り決めておき、アクセス許可条件リスト107の中に記入しておく。この場合、例えば、ホームシステム2のアクセス許可条件リスト107の中には、図19のようなデータが入っている。

【0218】例えば、ユーザ田中さんは、遠隔システム4を利用しており、ホームシステム2のファイルをコピーしたいとき、リモートファイル転送プログラムを利用する。この時の手順は、以下のような処理e-1〜処理e-14となる。なお、この手順にて交換される情報の流れを、図25に示す。

【0219】処理e-1 ユーザ田中さんは、遠隔システム4のリモートファイル転送206（クライアント側）をユーザID=101の権限として起動させる。

【0220】処理e-2 そのプログラムは、外部アクセス検出部101、コネクション管理部102、ネットワーク部103、LAN111を経て相手計算機システム（ホームシステム2）と通信路を設定し（IPデータグラム通信が可能になる）、TCPのコネクション設定を要求する。本実施の形態では、クライアント側の外部

【0221】処理e-3 相手計算機システム（ホームシステム2）のネットワーク部103を通り、コネクション管理部102へ要求がくる。

【0222】処理e-4 相手計算機システム（ホームシステム2）のコネクション管理部102では、発信元計算機システム（遠隔システム4）とのTCPのコネクションを張り、外部アクセス検出部101を通り、リモートファイル転送206（サーバ側）を起動しようとする。

【0223】処理e-5 ホームシステム2の外部アクセス検出部101は、上記のコネクション要求を検出し、接続の可否の判断を外部アクセス許可判断部106Bに依頼する。外部アクセス許可判断部106Bでは、コネクション管理部102へ、発信元計算機システム（遠隔システム4）のネットワークアドレスとユーザIDを要求する。

【0224】処理e-6 上記コネクション管理部102では、トランスポートレイヤのコネクションを張る段階で発信元計算機システム（遠隔システム4）のネットワークアドレスやコネクション識別子（ポート番号）が得られている。これは、TCPのプロトコルの仕様に基づくものである。

【0225】処理e-7 ホームシステム2の外部アクセス許可判断部106Bでは、さらに、発信元計算機システム（遠隔システム4）のユーザ・コネクション対応管理部211に問い合わせることにより、このコネクションを張った発信元計算機システム（遠隔システム4）のユーザIDなどの情報が得られる。このユーザ・コネクション対応管理部211の処理は、identificationブ

ロトコル（RFC1413などで規定）に従って行われているものである。

【0226】処理e-8 さらに、ユーザIDなどを返答する際に、返答データを署名・認証部108にて、自システム（遠隔システム4）の秘密鍵で暗号化して遠隔システム4の署名を付加してから返答する。この返答データの中には送信元システム（遠隔システム4）のネットワークアドレスが平文で含まれている。

【0227】処理e-9 受信側計算機システム（ホームシステム2）の外部アクセス検出部101は、上記発信元計算機システム（遠隔システム4）のユーザ・コネクション対応管理部211からの署名付きデータを署名・認証部108にて認証したのち、2つのデータ（発信元ネットワークアドレスとユーザID）を得る。

【0228】処理e-10 ホームシステム2の署名・認証部108では、上記認証は、発信元計算機システム（遠隔システム4）の公開鍵を公開鍵取得部110にて取得し、この公開鍵でデータを復号し、その結果が平文で送られてきたネットワークアドレスと一致することで復号が成功し、認証される。成功すると、返答データから発信元システムのネットワークアドレスやユーザIDなどの情報が平文で得られる。

【0229】処理e-11 得られたデータが前述のアクセス許可条件リスト107に登録されているか検索を行う。ここで、更にアクセス条件が付加されていれば（時間など）、それも考慮してアクセス可能か否かをチェックする。その可否と、可能な場合の、自システムにおけるユーザIDを外部アクセス検出部101へ伝える。

【0230】処理e-12 外部アクセス検出部101では、検査に合格すると、対応している自システム（ホームシステム2）のユーザID（この場合ユーザID=1）と起動させるプログラム名などをユーザID変換部104Bへ伝え、ここで指示された権限で、リモートファイル転送206（サーバ側）を動作させ、発信元計算機システム（遠隔システム4）のリモートファイル転送206（クライアント側）とコネクションを張り、リモートコピーの処理を開始する。この場合、第2、3の実施の形態と異なり、既に認証が済んでいるので、再度ログイン処理をしないで、認証できた自システム（ホームシステム2）のユーザID（この場合、ユーザID=1）の権限で、アクセス制御を行うことができる。ただし、第2、3の実施の形態のように、再度ログイン処理を行っても構わない。

【0231】処理e-13 外部アクセス許可判断部106Bで不可の判断が出ると、外部アクセス検出部101では、発信元計算機システム（遠隔システム4）に不許可の返事を返し、コネクションの切断をコネクション管理部102へ指示する。

【0232】処理e-14 合格した場合、遠隔システ

ム 4 のユーザは、実際のファイル転送の処理を利用可能になる。

【0233】リモートログインプログラムの場合も同様に、外部の計算機システム（遠隔システム 4）のネットワークアドレスとユーザ ID で認証を行ってから、対応する自システムのユーザ ID を求め、そのユーザ ID のアクセス権限でリモートログインの処理を行う。

【0234】以上説明したように、本実施の形態によれば、管理や計算機システムの構成の異なる複数の計算機システムをネットワークを介して接続した分散環境において、各計算機システムでユーザ管理やファイル管理が異なるのにも関わらず、ユーザが移動した先の計算機システムにおいて安全にファイルなどの個人情報を扱えるので、地理的に分散した環境下でも効率よい個人作業支援が可能になる。

【0235】すなわち、従来、ユーザが外部から計算機システムを利用する場合、計算機システム間のユーザ ID 管理が独立していると、同一ユーザであっても別々のユーザ ID を利用しなければならず、不便であった。さらに、互いの計算機システムが広域ネットワークに接続されていると、通信相手を信用することが困難であり、外部からの利用は、再度、ログイン処理を行ってユーザ確認を行うなど、ユーザに手間をかけていた。

【0236】本実施の形態では、ユーザ ID の対応関係を予め、計算機システム間で交換しておき、計算機システム間の認証機能を付加することにより、ユーザの外部からの利用の際には、計算機システム間で認証を行うだけで、同一ユーザのユーザ ID 対応関係が得られるので、ユーザに認証や、他マシンでのユーザ ID の入力やパスワードの入力を求めることなく、自動的にユーザ ID の対応関係の取得とユーザ ID の変換を行うことが可能になり、互いにユーザ管理が異なるシステムであってもユーザにとっては、再ログイン等の不便さが大幅に軽減されるという効果が得られる。

【0237】尚、上記第 4 の実施の形態では、リモートファイル転送 206 を例にとり説明したが、この実施の形態は直接ユーザがファイル転送を行う場合にも利用できる。例えば、Sun Microsystems 社のネットワークファイルシステム（NFS）のプロトコルに従ってファイルアクセスを行う場合、マウント処理の時に両計算機システム間で計算機システムの認証を行い、両システム間のユーザ ID の対応関係を得る。以後、ファイルアクセス命令のパケットごとに、ユーザ ID 変換部 104 B でユーザ ID を対応したものに replacement と、遠隔システム 4 から利用してもホームシステム 2 で利用したのと同様なアクセス制御が可能となる。

【0238】又、上記第 4 の実施の形態では、ユーザ ID の変換処理をホームシステム 2（サーバ）側で行ったが、遠隔システム 4（クライアント）側で行ってもよい。

【0239】また、本発明は上述した各実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【0240】

【発明の効果】本発明によれば、管理や構成の異なる複数の計算機をコントロール・ネットワークを介して接続した分散環境において、ユーザが 1 つの計算機を他の計算機から利用する場合でも、該 1 つの計算機における資源を、そこでのユーザ識別情報（のアクセス権限）を用いて利用することが可能である。しかも、該 1 つの計算機でのユーザ識別情報をほとんど意識することなく、他の計算機（のユーザ識別情報）から利用することができる。

【0241】また、管理や構成の異なる場合、通常、外部からの不正アクセスを防ぐため、外部のアクセスは厳しく制限されているが、本システムによって、外部からのアクセスは、許可された計算機システムとユーザにだけ可能になり、その管理も容易となる。

【0242】したがって、各計算機でユーザ管理やファイル管理が異なるのにも関わらず、ユーザが移動した先の計算機システムにおいて安全に通信ができ、かつ、ファイル等の個人情報を扱えるので、地理的に分散した環境下でも効率よい個人作業支援が可能になる。

【図面の簡単な説明】

【図 1】本発明のシステムの全体構成を示す概略ブロック図。

【図 2】本発明の第一の実施の形態における図 1 のシステムの各計算機システム（ホームシステム、遠隔システム）の機能的構成を示すブロック図。

【図 3】本発明のシステムの別の全体構成を示す概略ブロック図。

【図 4】図 3 のシステムのセキュリティゲートウェイの機能的構成を示すブロック図。

【図 5】図 3 のシステムのセッション情報管理サーバの機能的構成を示すブロック図。

【図 6】図 3 のシステムのホームシステムの機能的構成を示すブロック図。

【図 7】図 9 のシステムのフィルタリングルータの機能的構成を示すブロック図。

【図 8】図 9 のシステムのネットワークデータ処理サーバの機能的構成を示すブロック図。

【図 9】図 3 のシステムの変形構成例を示すブロック図。

【図 10】図 1 のシステムのクライアント側計算機システムのセッション設立動作における機能的構成を示すブロック図。

【図 11】図 1 のシステムのサーバ側計算機システムのセッション設立動作における機能的構成を示すブロック図。

【図 12】図 11 のサーバ側計算機システムでのセッシ

ョン設立動作で使われるアクセス許可条件リストを示す図。

【図13】図11のサーバ側計算機システムでのセッション設立動作でセッション情報保存部に保存されるセッション情報を示す図。

【図14】図1のシステムの計算機システムのセッションを使った通信時における機能的構成を示すブロック図。

【図15】本発明の第二の実施の形態におけるシステムの名計算機システム（ホームシステム、遠隔システム）の機能的構成を示すブロック図。

【図16】図15の計算機システムの個人スケジュール管理部で使われるスケジュール管理表を示す図。

【図17】図15の計算機システムで使われるアクセス許可条件リストを示す図。

【図18】図15の計算機システムで使われるユーザID共通化要求データを示す図。

【図19】図15の計算機システムのユーザID対応管理表に格納されるアクセス許可データを示す図。

【図20】本発明の第二の実施の形態における遠隔システムからのリモートファイル転送利用の手順を示すシーケンス図。

【図21】本発明の第三の実施の形態におけるシステムの名計算機システム（ホームシステム、遠隔システム）の機能的構成を示すブロック図。

【図22】図21の計算機システムで使われるユーザID共通化要求データを示す図。

【図23】図21の計算機システムで利用可能なネットワーク管理システムのデータベースを示す図。

【図24】本発明の第四の実施の形態におけるシステムの名計算機システム（ホームシステム、遠隔システム）の機能的構成を示すブロック図。

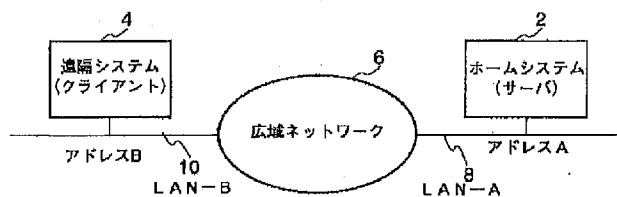
【図25】本発明の第四の実施の形態における遠隔システムからのリモートファイル転送利用の手順を示すシーケンス図。

【符号の説明】

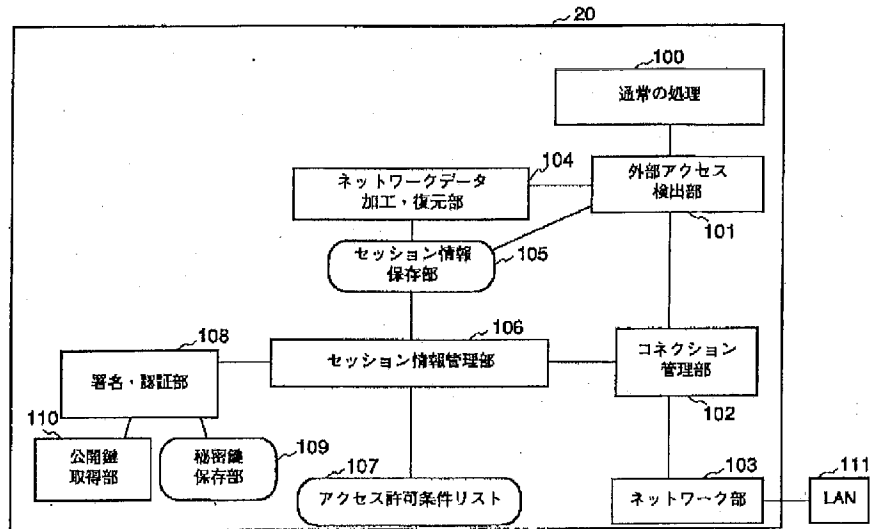
2, 60 ホームシステム

4 遠隔システム
6 広域ネットワーク
8, 10, 111 LAN
20, 150, 210, 240 計算機システム
30 ホームシステムグループ
40 セキュリティゲートウェイ
50 セッション情報管理サーバ
70 フィルタリングルータ
80 ネットワークデータ処理サーバ
90 ルータ
100 通常の処理
101 外部アクセス検出部
102 コネクション管理部
103 ネットワーク部
104 ネットワークデータ加工・復元部
104A ユーザID変換部
105 セッション情報保存部
105A ユーザID対応管理表
106 セッション情報管理部
106A ユーザID共通化部
106B 外部アクセス許可判断部
107 アクセス許可条件リスト
108 署名・認証部
109 秘密鍵保存部
110 公開鍵取得部
151 個人スケジュール管理部
152 一時的パスワード入力
153 一時的パスワード生成
201 入出力部
202 ローカルログイン
203 ユーザ管理部
204 リモートログイン
205 ファイルシステム
206 リモートファイル転送
211 ユーザ・コネクション対応管理部
212 計算機システム秘密鍵保存部
213 個人秘密鍵入力部

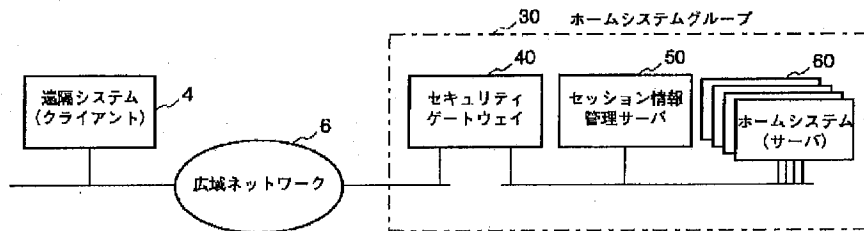
【図1】



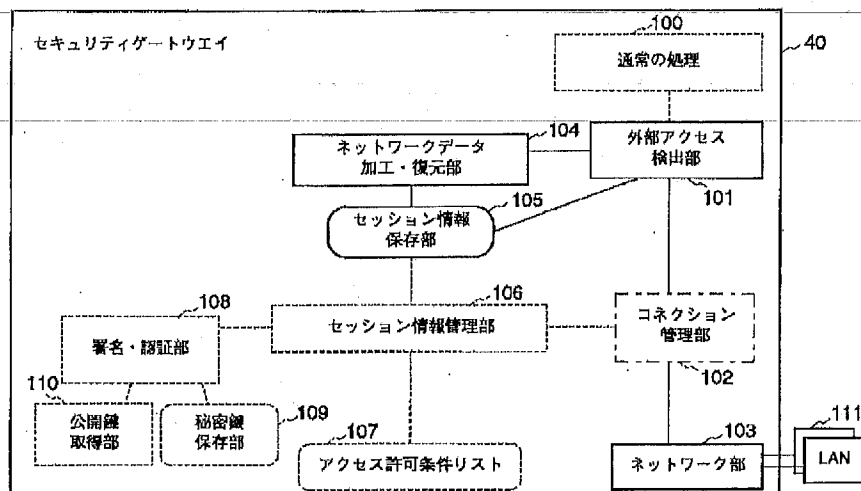
【図2】



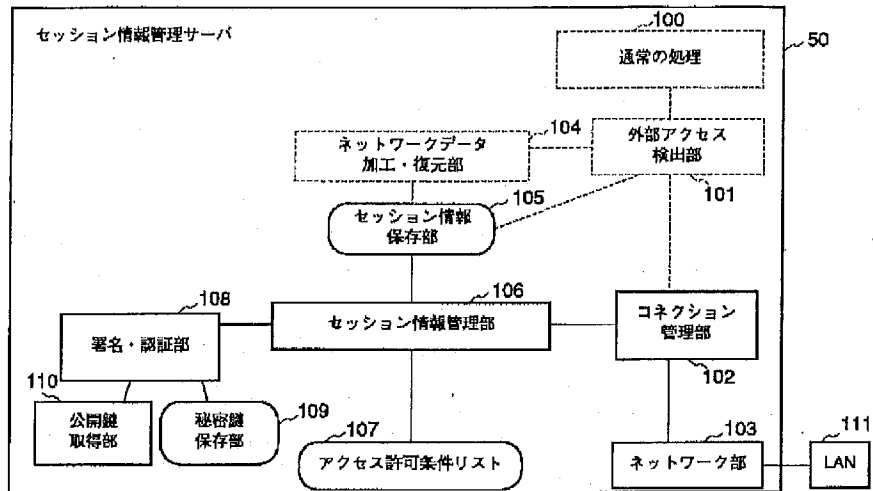
【図3】



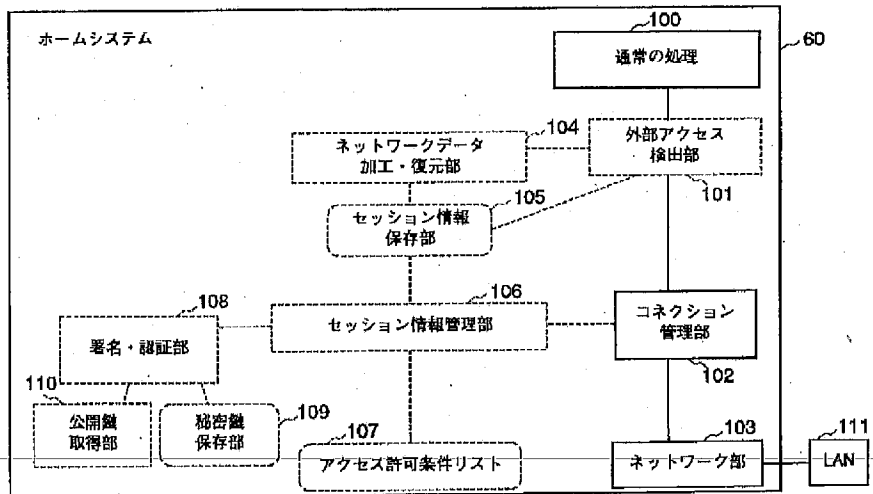
【図4】



【図5】



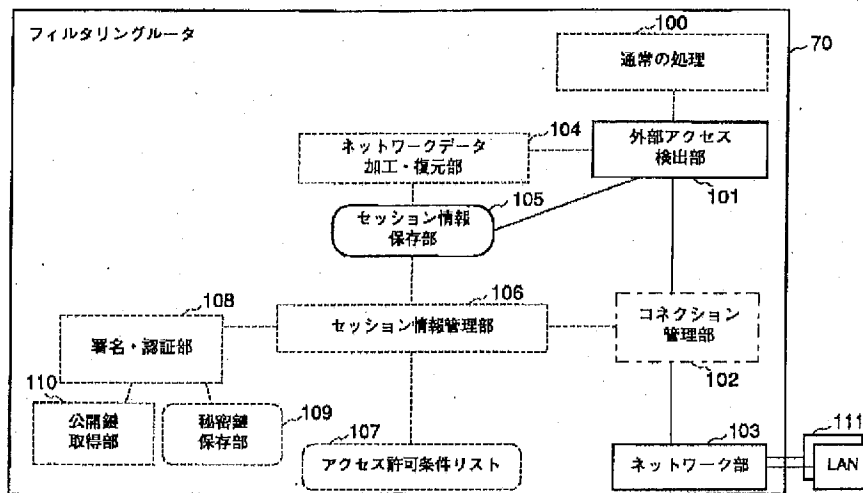
【図6】



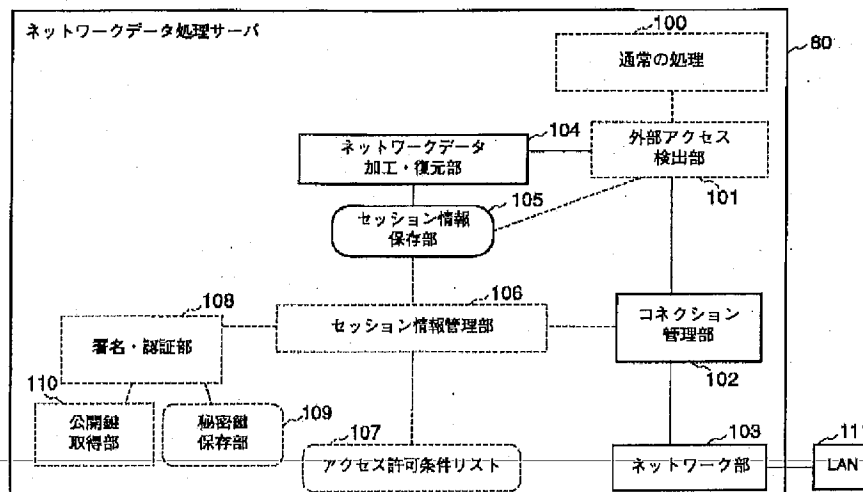
【図17】

ユーザ ID	外部システムの ネットワークアドレス	一時的パスワード	有効期間
1.	B	ABC123	1994.4.1 13:00~17:00
		⋮	
		⋮	
		⋮	

【図7】



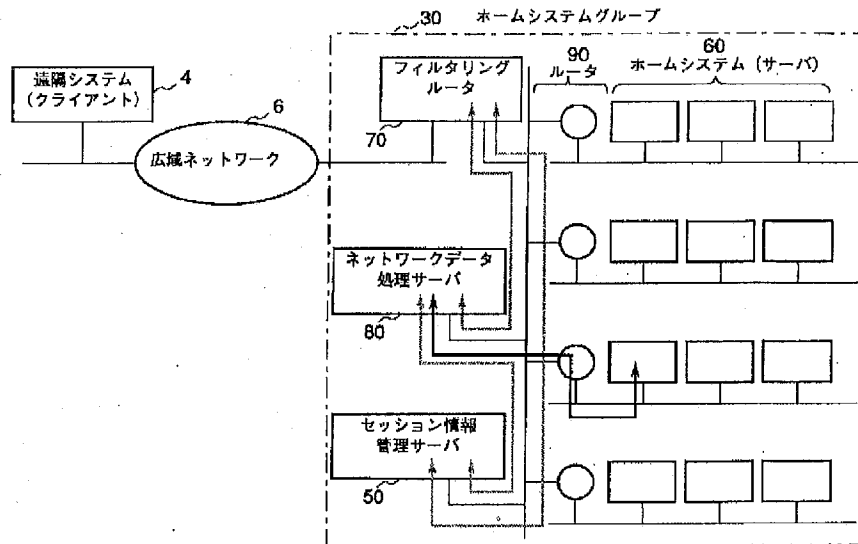
【図8】



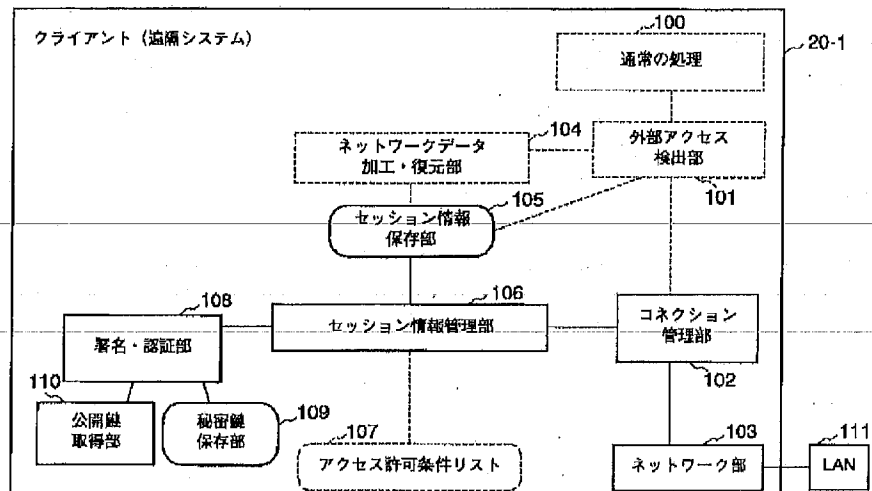
【図19】

自システム上の ユーザID	外部システムの ネットワークアドレス	外部システムの ユーザID	有効期間
1	B	101	1994.4.1 13:00~17:00

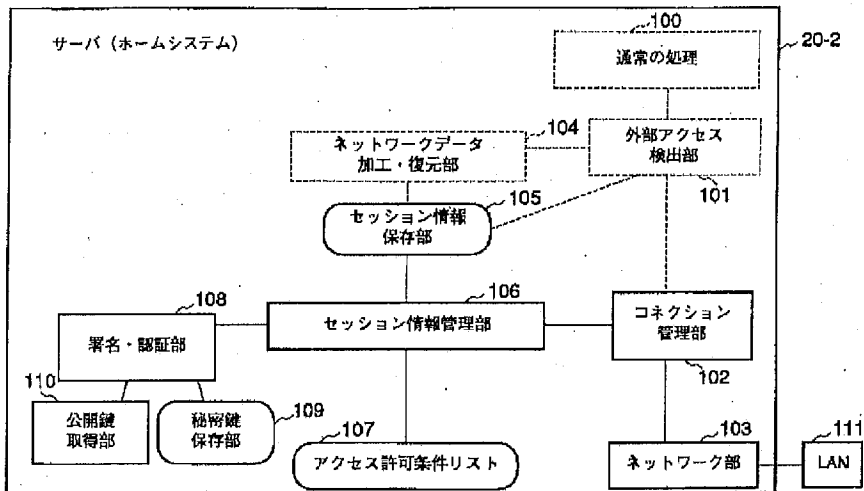
【図9】



【図10】



【図11】



【図12】

【図18】

ユーザ ID	許可する外部システムのネットワークアドレス	有効期間	その他の条件
1	B	UNTIL 1995.12.31	
2	A~D	1995.1.1~1995.12.31	
3	ALL	ANY TIME	
4	C	1995.9.1 9:00~17:00	TELNET,FTP のみ
5	NONE	NONE	
		.	
		.	
		.	

ユーザID共通化用データである旨の識別子
送信元ネットワークアドレス
あて先ネットワークアドレス
送信元の計算機システムでのユーザID
あて先の計算機システムでのユーザID
一時的パスワード

【図23】

ネットワークアドレス	システム名	設置場所
1000	本社	東京都港区
1001	川崎支店	川崎市川崎区
1002	研究所	川崎市幸区
1003	大阪支店	大阪市北区
2000	会議室 A	本社9階
2001	会議室 B	本社8階
2002	会議室 C	本社7階

【図13】

自システムの ユーザ ID	許可した外部 システムのネット ワークアドレス	許可した外部 システムの ユーザID	セッション鍵	セッション ID	有効期間	その他の条件
1	B	101	ABCDEF	1	UNTIL 1995.12.31	
3	F	43	QWERTY	2	ANY TIME	
4	C	67	ZXCVBN	3	1995.9.1 9:00~17:00	TELNET,FTP のみ
			⋮		⋮	
			⋮		⋮	
			⋮		⋮	

【図14】

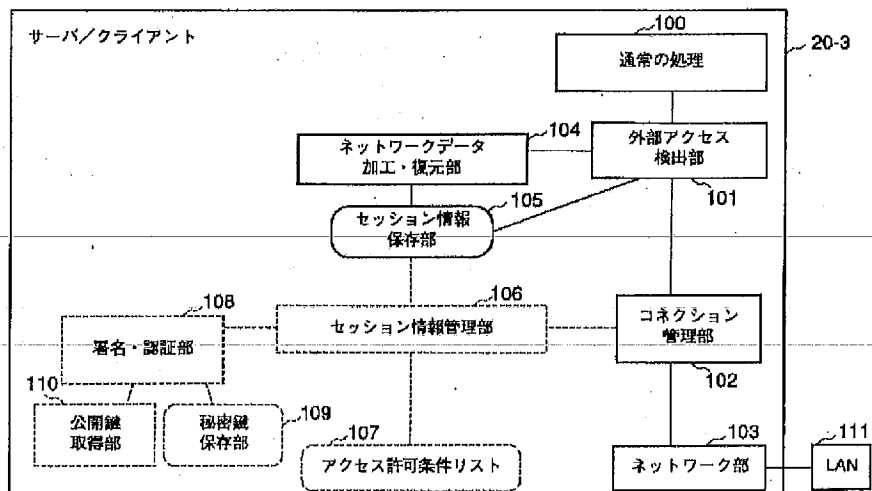
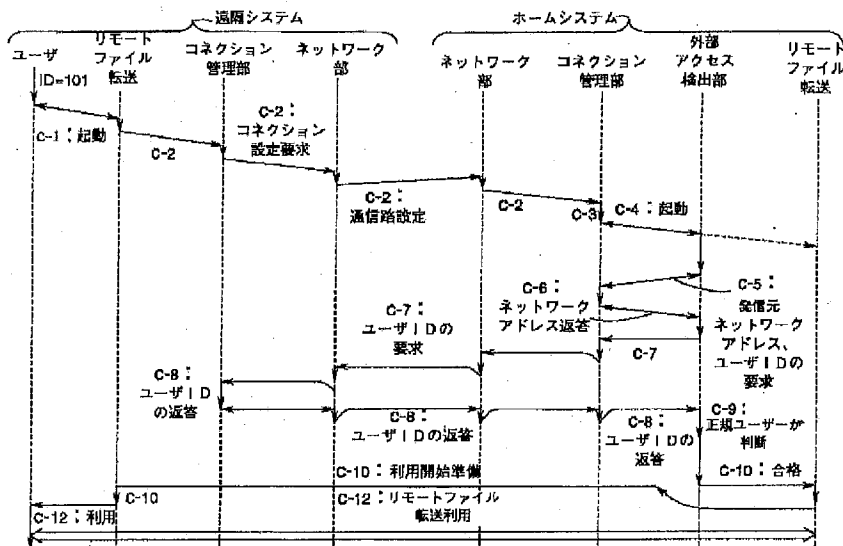


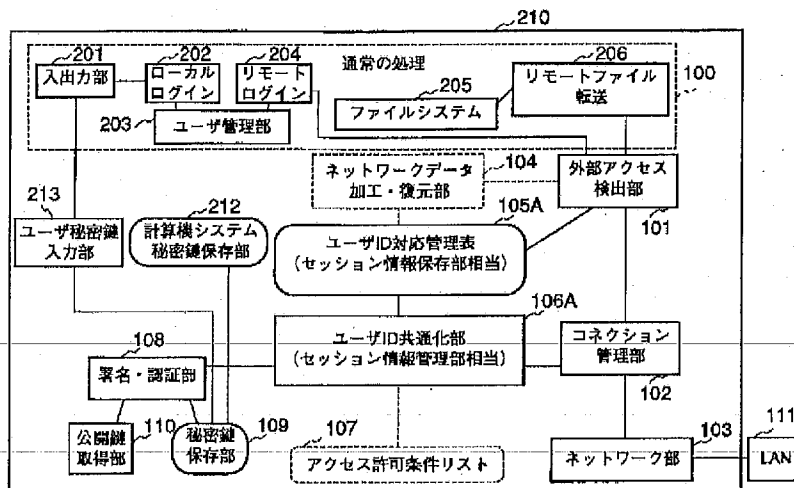
Figure 1 is a block diagram of the system architecture. The diagram shows a central 'ユーザID対応管理表 (セッション情報保存部相当)' (105A) connected to various components. On the left, '201 入出力部' connects to '202 ローカルログイン' and '204 リモートログイン'. '202' connects to '203 ユーザ管理部', which connects to '個人スケジュール管理部' (151) and '一時的パスワード入力' (152). '152' connects to '一時的パスワード生成' (153), which connects to '署名・認証部' (108). '108' connects to '公開鍵取得部' (110) and '秘密鍵保存部' (109). '109' connects to 'アクセス許可条件リスト' (107). '107' connects to 'ユーザID共通化部 (セッション情報管理部相当)' (106A), which connects to 'コネクション管理部' (102). '102' connects to 'ネットワーク部' (103), which connects to 'LAN' (111). '105A' also connects to 'ネットワークデータ加工・復元部' (104), which connects to '外部アクセス検出部' (101). '101' connects to 'リモートファイル転送' (206), which connects to 'ファイルシステム' (205). '205' connects to '通常の処理' (150). '150' connects to '206'.

日 時	場 所	ネットワーク アドレス
94-4-1	ホームシステム	A
	移動中	-
	通隔システム	B

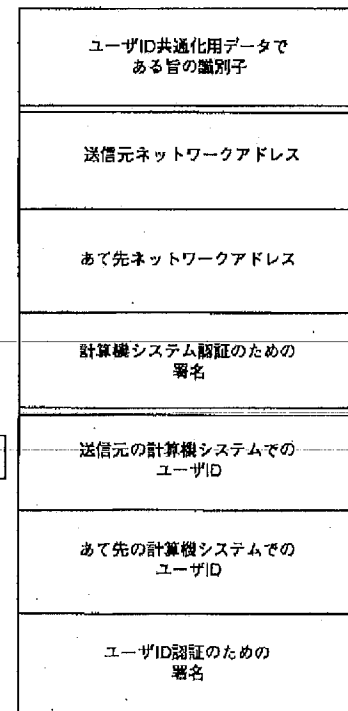
【図20】



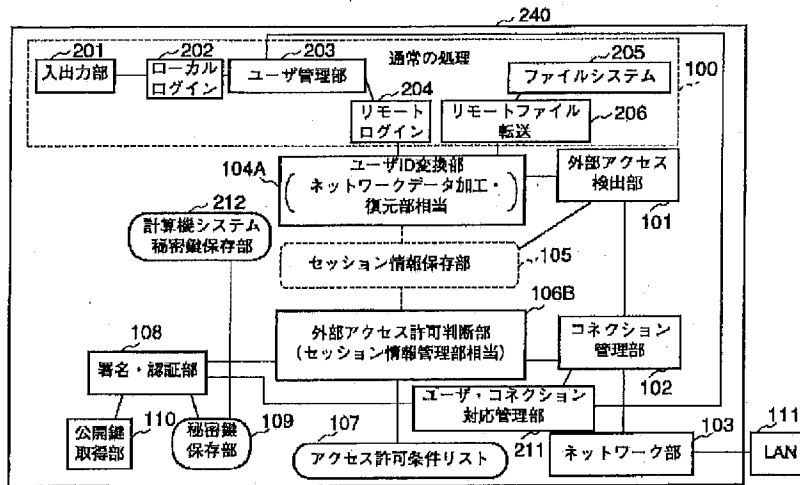
【図21】



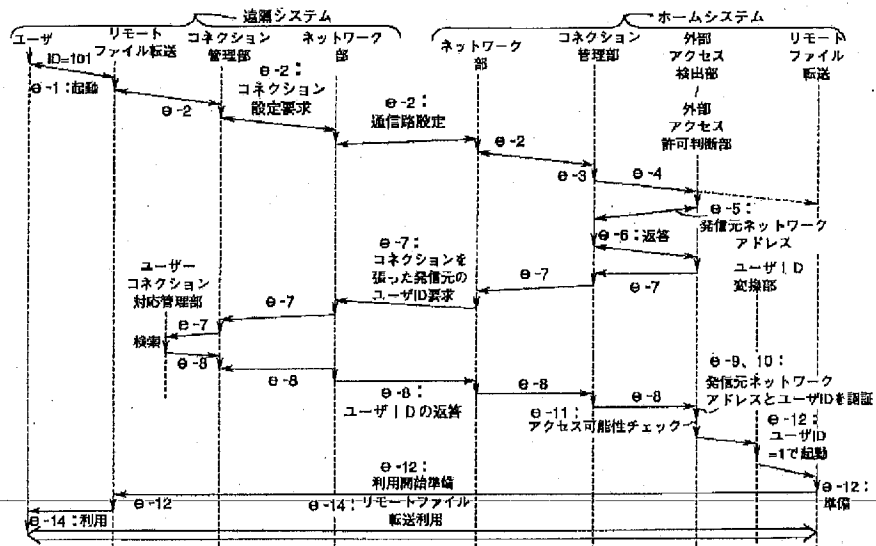
【図22】



【図24】



【図25】



フロントページの続き

(51) Int. Cl. 6

H 0 4 L 9/14

識別記号

片内整理番号

F I

技術表示箇所

C8-19

【公報種別】特許法第17条の2の規定による補正の掲載
【部門区分】第6部門第3区分
【発行日】平成14年3月12日(2002. 3. 12)

【公開番号】特開平8-153072
【公開日】平成8年6月11日(1996. 6. 11)
【年通号数】公開特許公報8-1531
【出願番号】特願平7-255169
【国際特許分類第7版】

G06F 15/00 330

G09C 1/00
H04L 9/06
9/14

【F I】

G06F 15/00 330 B
330 C

G09C 1/00
H04L 9/02 Z

【手続補正書】

【提出日】平成13年10月30日(2001. 10. 30)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 通信手段により互いに接続されて互いに通信可能な複数の計算機を有する計算機システムであって、該複数の計算機のうち少なくとも一つの計算機は不正なアクセスから保護されており、該システムが、他の計算機から該少なくとも一つの計算機へのアクセス要求が許可されるべきかどうかを該他の計算機が前記複数の計算機の内のどれかに基づいて判断し、該少なくとも一つの計算機への通信がそこから該少なくとも一つの計算機へのアクセスが許可された前記複数の計算機中のある計算機からのものかどうか検査するのに用いられるアクセス許可データを生成する管理手段と、該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、を有することを特徴とする計算機システム。

【請求項2】 前記管理手段は、前記アクセス要求が許可されるべきかどうかを該アクセス要求を行ったユーザにも基づいて判断し、前記通信が前記少なくとも一つの計算機へのアクセスが許可されたあるユーザからのものかどうか検査するのに用いられる前記アクセス許可データを生成することを特徴とする請求項1記載の計算機システム。

【請求項3】 前記少なくとも一つの計算機にアクセスすることを許可されるべきユーザと計算機の全ての組み合わせを示すアクセス許可条件を格納する格納手段を更に有し、該アクセス許可条件のは前記少なくとも一つの計算機における前記あるユーザのユーザ識別情報を指定し、前記管理手段は該格納手段に格納された該アクセス許可条件に基づいて、該アクセス許可条件を前記アクセス要求が示す前記少なくとも一つの計算機における前記ユーザのユーザ識別情報と比較することにより判断することを特徴とする請求項2記載の計算機システム。

【請求項4】 前記アクセス許可条件は更に前記ある計算機のシステム識別情報を指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機のシステム識別情報と比較することにより判断することを特徴とする請求項3記載の計算機システム。

【請求項5】 前記アクセス許可条件は更に前記ある計算機における前記あるユーザの一時的パスワードを指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機における前記ユーザの一時的パスワード比較することにより判断することを特徴とする請求項3記載の計算機システム。

【請求項6】 前記アクセス許可条件は更に前記他の計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記少なくとも一つの計算機におけるユーザのユーザ識別情報及び該有効期間を含んだ前記アクセス許可データを生成することを特徴とする請求項3記載の計算機システム。

【請求項7】 前記アクセス要求は、発信元システム識別情報、発信先システム識別情報、及びシステム識別署名データを示し、前記管理手段は該システム識別署名データを認証することにより判断することを特徴とする請求項1記載の計算機システム。

【請求項8】 前記少なくとも一つの計算機におけるあるユーザのユーザ識別情報を示すアクセス許可条件を格納する格納手段を更に有し、前記アクセス要求は、発信先ユーザ識別情報及びユーザ識別署名データを示し、前記管理手段は該ユーザ識別署名データを認証し、該発信先ユーザ識別情報を該格納手段に格納された該アクセス許可が示す該ユーザ識別情報と比較することにより判断することを特徴とする請求項2記載の計算機システム。

【請求項9】 前記アクセス要求は更に、発信元ユーザ識別情報も示し、前記ユーザ識別署名データは、前記発信元ユーザ識別情報と前記発信先ユーザ識別情報を前記ユーザの秘密鍵を使って暗号化して求められたものであり、前記管理手段は該ユーザ識別署名データを前記ユーザの公開鍵を使って復号化することにより認証することを特徴とする請求項8記載の計算機システム。

【請求項10】 前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機のシステム識別情報及び前記他の計算機における前記ユーザのユーザ識別情報を含んだ前記アクセス許可データを生成することを特徴とする請求項9記載の計算機システム。

【請求項11】 前記アクセス許可条件は更に前記他の計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を更に含んだ前記アクセス許可データを生成することを特徴とする請求項10記載の計算機システム。

【請求項12】 前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機から前記ユーザによる前記各計算機への通信に使われる鍵データを含んだ前記アクセス許可データを生成することを特徴とする請求項1記載の計算機システム。

【請求項13】 該少なくとも一つの計算機への通信が該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して前記他の計算機から間接的になされたものかを検出し、該通信が間接的になされたものである場合、該通信が正当なアクセスであるかどうかを前記メモリ手段に記憶した前記アクセス許可データに基づいて検査して正当なアクセスを許可する検出手段と、を有することを特徴とする請求項1記載の計算機システム。

【請求項14】 前記メモリ手段は、前記ある計算機における前記あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報との組を記憶し、

前記検出手段は、前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を前記メモリ手段が記憶しているとき、前記アクセスを正当と判定することを特徴とする請求項13記載の計算機システム。

【請求項15】 前記メモリ手段は更に、前記ある計算機における前記あるユーザのための前記アクセス許可データに対応する鍵データを記憶し、前記少なくとも一つの計算機は更に、前記検出手段が該アクセス許可データに基づいて前記アクセスを正当と判定したとき、前記アクセスの通信データを前記鍵データを使って加工するデータ加工手段を有することを特徴とする請求項13記載の計算機システム。

【請求項16】 前記メモリ手段は更に、前記他の計算機におけるあるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を記憶し、前記検出手段は、該メモリ手段に記憶した該有効期間に基づいて、前記アクセスを正当と判定することを特徴とする請求項13記載の計算機システム。

【請求項17】 複数の計算機群がネットワークにより互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機群のうち少なくとも一つの計算機群が、他の計算機群の計算機から該少なくとも一つの計算機群の計算機へのアクセス要求が許可されるべきかどうかを該他の計算機群が前記複数の計算機群の内のどれかに基づいて判断し、該少なくとも一つの計算機群の計算機への通信がそこから該少なくとも一つの計算機群の計算機へのアクセスが許可された前記複数の計算機群の内の一計算機群の計算機からのものかどうか検査するのに用いられるアクセス許可データを生成するデータ管理サーバと、

前記データ管理サーバにより生成された該アクセス許可データに対応して鍵データを記憶するメモリ手段と、該少なくとも一つの計算機群の計算機への通信が正当なアクセスであるかどうかを前記アクセス許可データに基づいて検査して正当なアクセスを許可するとともに、正当なアクセスの通信データを前記鍵データを使って加工する手段と、を含むセキュリティゲートウェイと、を有することを特徴とする計算機システム。

【請求項18】 複数の計算機がネットワークにより互いに接続されて互いに通信可能に構成された計算機システムにおける計算機であって、他の計算機から該計算機へのアクセス要求が許可されるべきかどうかを該他の計算機が前記複数の計算機の中のどれかに基づいて判断し、該計算機への通信がそこから該計算機へのアクセスが許可された前記複数の計算機中の一つからのものかどうか検査するのに用いられるアクセス許可データを生成する管理手段と、

該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、を有することを特徴とする計算機。

【請求項19】 複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、

該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを判定し、正当と判定された場合、該アクセスを許可する検出手段と、

そこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユー

ザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報と、該あるユーザの該少なくとも一つの計算機における内部ユーザ識別情報との組を記憶するメモリ手段であって、前記検出手段は前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を該メモリ手段が記憶しているとき前記アクセスを正当と判定するものと、

前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データが示すユーザ識別情報を該ユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記内部ユーザ識別情報に変換する変換手段と、を有することを特徴とする計算機システム。